NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERCIEGE SCENARIO ILLUSTRATING SOFTWARE INTEGRITY ISSUES AND MANAGEMENT OF AIR-GAPPED NETWORKS IN A MILITARY ENVIRONMENT

by

Chay Chua

December 2005

Thesis Co-Advisors:	Cynthia E. Irvine
	Paul C. Clark
Second Reader:	Michael F. Thompson

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, 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, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE December 2005	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: CyberCIEGE Scenario Illustrating Software Integrity Issues and Management of Air-Gapped Networks In A Military Environment		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Chay Chua			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The importance of Information Assurance (IA) in military operations cannot be overstated. It is a *sine qua non* that achieving IA requires the effort of all personnel in the organization; just a single untrained end-user is needed to defeat many well thought-out and well-executed security strategies This thesis demonstrated that CyberCIEGE, with its rich elements and tools, can be used to create game scenarios, mimicking real life IA issues, for conveying security lessons to a wide audience of trainees. It provides an excellent alternative to the traditional methods of security education which so often fail in driving home the intended lessons.

A military-based CyberCIEGE scenario definition file (SDF) was developed to illustrate and train players on the importance of ensuring hardware and software integrity in operational-critical systems. The focus of the research was on the protection of sensitive information systems through the maintenance of their software integrity and the application of an air-gapped network architecture. The test cases developed in this thesis research also contributed to the improvement of the CyberCIEGE game engine.

14. SUBJECT TERMS CyberCIEGE, Information Assurance, Computer Security, Information Security, Security Training Integrity, Air-gapped Network, Software Integrity, Hardware Integrity, Scenario Definition File			15. NUMBER OF PAGES 100
			16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

THIS PAGE INTENTIONALLY LEFT BLANK

CYBERCIEGE SCENARIO ILLUSTRATING SOFTWARE INTEGRITY ISSUES AND MANAGEMENT OF AIR-GAPPED NETWORKS IN A MILITARY ENVIRONMENT

Chay Chua
Captain, Singapore Armed Forces
B.Eng. (Hons), University of Sheffield in United Kingdom, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

**NAVAL POSTGRADUATE SCHOOL
December 2005**

Author: Chay Chua

Approved by: Cynthia E. Irvine
                     Thesis Co-Advisor

                     Paul C. Clark
                     Thesis Co-Advisor

                     Michael F. Thompson
                     Second Reader

                     Peter J. Denning
                     Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The importance of Information Assurance (IA) in military operations cannot be overstated. It is a *sine qua non* that achieving IA requires the effort of all personnel in the organization; just a single untrained end-user is needed to defeat many well thought-out and well-executed security strategies This thesis demonstrated that CyberCIEGE, with its rich elements and tools, can be used to create game scenarios, mimicking real life IA issues, for conveying security lessons to a wide audience of trainees. It provides an excellent alternative to the traditional methods of security education which so often fail in driving home the intended lessons.

A military-based CyberCIEGE scenario definition file (SDF) was developed to illustrate and train players on the importance of ensuring hardware and software integrity in operational-critical systems. The focus of the research was on the protection of sensitive information systems through the maintenance of their software integrity and the application of an air-gapped network architecture. The test cases developed in this thesis research also contributed to the improvement of the CyberCIEGE game engine.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAF	Alliswell Armed Forces
ARILS	AAF Real-time Integrated Logistics System
CO	Commanding Officer
DAC	Discretionary Access Control
DARPA	Defense Advanced Research Projects Agency
DOD	Department Of Defense
HQ	Headquarter
LAN	Local Area Network
MAJ	Major
SAF	Singapore Armed Forces
SDF	Scenario Definition File
SDT	Scenario Development Tool
SGT	Sergeant
WO	Warrant Officer

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Many individuals have provided me with positive influence and assistance during my course of studies in NPS and the development of this thesis. I would like to take this opportunity to express my deepest appreciation to them.

I would especially like to thank my wife, Mandy, for her understanding and unwavering support, through my many long hours of work away in school, and at home. Your love and support have provided me the energy to soldier on during the toughest of time.

I would like to express my sincere gratitude to Dr. Cynthia Irvine, Paul Clark, and Mike Thompson, my advisors for this thesis work. Thank you for your patience, guidance and constructive critique.

Finally, I would like to express my special thanks to Nai Kwan, Chee Mun, Chris Lim, Sitthichai and Carl Lee for their friendship and camaraderie. You have helped to make my one year graduate studies at NPS and my stay in Monterey such a wonderful experience.

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

This chapter introduces the topic of this research and introduces the scope and outline of the remainder of the document.

A.   THESIS STATEMENT

The purpose of this thesis was to investigate how CyberCIEGE can be used as a tool for security educational where the objective is to improve the security awareness level of personnel in an organization that has demanding needs for integrity of critical operational networks. CyberCIEGE is "a high-end, commercial-quality video game developed jointly by Rivermind and the Naval Postgraduate School's Center for Information Systems Security Studies and Research" (Irvine 2005, 2).

The research focused on the development of a CyberCIEGE Scenario Definition File (SDF) that is intended to mimic real life Information Assurance (IA) issues and educate the players on integrity issues found in a military environment.

This research aimed to answer the following three questions:

1.   First Question

Can a scenario be developed such that it is both playable and educational while illustrating the need for security and protection of mission critical data in a networked military environment?

2.   Second Question

Can a scenario illustrate the tensions, trade-offs and decisions a network manager has to make when deciding between the use of an air-gapped network that is separated from the Internet and the need for web connectivity?

3.   Third Question

From the perspective of information assurance, to what extent is the use of commercial software on an air-gapped network comparable to connecting the network to the Internet, in terms of subjecting the network to possible malicious acts by adversaries?

This thesis contributes to the ongoing research and development of the CyberCIEGE project at the Naval Postgraduate School.

B.   THESIS SCOPE AND LAYOUT

The scope of the thesis is to create a CyberCIEGE SDF that can be used to educate DoD personnel and intermediate level computer science students on security topics such as the importance of maintaining physical network isolation of critical backbone networks; the integrity of commercial software; and the controlled movement of information from a low integrity network to a high integrity network.

This thesis comprises the following chapters:

1.   Chapter I - Introduction

This introductory chapter provides the thesis statements and describes the scope and layout of the thesis.

2.   Chapter II - Background

This chapter covers the background information that establishes a framework for scenario development and provides readers with an overview of computer security and the current information security training situation. It also describes how CyberCIEGE can be used as an effective security training tool and highlights the importance of integrity in military systems.

3.   Chapter III – Scenario Strategy

This chapter discusses how CyberCIEGE can be used as a security educational tool to improve the security awareness level of personnel in an organization that has demanding needs for integrity of mission-critical networks.

4.   Chapter IV - Scenario Description

This chapter describes in detail the implementation of the scenario strategies to create a SDF that can be used to convey security lessons about the need for software integrity and an air-gapped network architecture in a sensitive military environment.

5.   Chapter V – Scenario Testing

This chapter discusses the test objectives and methodologies applied to verify the correctness of the Operation Artemis scenario. It also covers the informal testing

conducted during the scenario development process,which contributed to the improvement of the SDT and the CyberCIEGE game engine.

6.   Chapter VI – Conclusion and Recommendations

This is the final chapter of the thesis. It provides recommendations, suggests future work for the CyberCIEGE project and concludes the thesis.

C.   SUMMARY

In this chapter the thesis statement and the scope of the thesis are defined. Readers are also provided with an outline of the thesis and a brief description of the contents of each chapter in the thesis. Subsequent chapters will further develop the topics covered in this introductory chapter and attempt to answer the questions posed.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

This chapter covers the background information that establishes a framework for scenario development. It is intended to provide the readers an overview of computer security and an overview of the current information security training situation. It describes how CyberCIEGE can be used as an effective security training tool, and highlights the importance of integrity in military systems. The chapter also depicts the contribution of the thesis to the overall goal of the CyberCIEGE project and elaborates on computer security issues - such as the use of commercial software in mission critical systems and the application of air-gapped networks to reduce the risk of outsider attacks.

A. THE PAST, THE PRESENT, AND THE FUTURE OF CYBER SECURITY

The Internet emerged from a research program initiated by the United States Defense Advanced Research Projects Agency (DARPA) in 1973 for the development of communication protocols to enable interaction between networked computers (Cerf 2004). This research program was known as the Internetting project, and the resulting systems of networks were called ARPAnet, which eventually grew into today's Internet (Leiner 2003). During its infancy in the early 70s, computing power and knowledge were still limited to a privileged and trusted few, and computer security was not yet a pressing and popular concern. This was to change with the vast proliferation of microcomputers. The introduction of personal computers by Apple and IBM coupled with the introduction of global Internet in the late 70s and early 80s provided computing resources to the masses. These, however, also gave rise to a heightened awareness of computer security and information assurance issues, as they provided malicious users a springboard to learn and execute their crafts of cracking systems.

Cyber security is a concern in today's wired world. Kessler (1997) states:

In an ideal world, there would be no need for network or computer security. There would be no threats to your information. No one would be trying to break into any of your systems. There would be no disgruntled employees, competitors would not be trying to steal your secrets, and people with the smarts necessary to break into computer systems and create viruses would be working on more constructive endeavors. Unfortunately, we do not live in an ideal world and, therefore, we do have

to be concerned with security, possible break-ins, viruses, attacks from the Internet, and even security breaches from inside our own network. (Kessler 1997)

The modern world greatly depends on the use of computers and computer networks. They are instrumental to the daily operations of companies, organizations, and government. The management and operation of a nation's critical systems and infrastructures - such as nuclear power plants, dams, air traffic control systems, and the financial and economic infrastructures are hugely dependent on the correct functioning of its computers and computer networks. Life today depends on information. While this has been true for centuries, it has never been as true since the invention of the modern digital computer and the birth of the Internet. In today's world, up-to-date and "correct information is the key to any successful endeavor." (Kessler 1997)

Information security and military operations are intertwined. The importance of information security to military operations cannot be overstated (Ryan 1997). History has shown that information is critical to the success or failure of battles, campaigns, and wars. Some of the tried and proven methods by military commanders and theoreticians in gaining ascendancy in battles and obtaining knowledge of an opponent's intentions include the capturing of the opponent's messengers and the interception of written war plans or messages from the opponent's signaling devices.

In the First World War, the Germans were able to obtain the Russian's operation plans and tactical orders when they exploited the Russian's battlefield communications. This gave the German army unparallel advantages over their opponents and as a result, the decisive victory by the German army over a Russian army that was twice its size at Tannenberg in August of 1914. The lesson from the Tannenberg battle to military commanders regarding the importance of information security was clear. When battlefield communication and information system security fails, the battle may be lost. The following extracts from Jackson (2002) provided a brief description of the battlefield situations at Tannenberg:

> The majority of the men did not know how to use the devices or understand how the substitution ciphers were used to code messages. Additionally, complete codes were not distributed to all the corps for fear of them being lost and/or captured by the Germans. Also, it took time to

print and distribute codebooks, and given the fact that there was a large degree of illiteracy among the enlisted men that made the codebooks virtually useless, there was little impetus to expend energy on producing them. As a result, all communications (telephone, telegraph, wireless, and messenger) would be transmitted in the clear. (Jackson 2002)

In the Second World War, information security failures on the part of the Axis powers provided the Allies an overwhelming advantage and contributed significantly to the outcome of the war. The following quotation from FCW2 (2005) depicts how the tides of the war changed when the secrecy of the Japanese communication was compromised:

> The Battle of Midway in June, 1942 was arguably the turning point of World War II in the Pacific rim. The victory hinged partly on U.S. code crackers' breaking JN25 naval cipher to learn that the Japanese planned to attack Midway. Adm. Chester Nimitz, commander of the U.S. Pacific fleet, sent two carrier task forces to Midway to ambush the Japanese Navy. (FCW2 2005)

State sponsored attacks are also not uncommon. "Governments have been known to clandestinely insert vulnerabilities into the software embedded in outsourced products for their adversaries" (IT Pro 2005). One classical example is the "Farewell Dossier" campaign which was coordinated by the US Central Intelligence Agency (CIA) in the early 1980s. The following paragraph summarizes the incident as described in IT Pro.

The "Farewell Dossier" campaign orchestrated by the CIA had the Russian spies deceived into stealing computer chips embedded with a software Trojan horse by the US. The Soviets had intended to use the stolen software to control the electromechanical devices that would regulate the flow of natural gas through the Trans-Siberian pipeline. The Soviets proceeded to use the chips without detecting the Trojan horse, and the malicious software adjusted the output control signals to the electromechanical devices to increase pressure in the pipeline, resulting in the equivalent of a 3-kiloton explosion. This disaster made it financially difficult for the Soviets to pursue their defense research that they had planned to fund with natural gas revenues, and subsequently led to the ending of the cold war era (IT Pro 2005). The following extracts from Safire (2004) also described the "Farewell Dossier" campaign:

The technology topping the Soviets' wish list was for computer control systems to automate the operation of the new, trans-Siberian gas pipeline. When we turned down their overt purchase order, the K.G.B. sent a covert agent into a Canadian company to steal the software; tipped off by Farewell, we added what geeks call a "Trojan Horse" to the pirated product… "The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire," writes Reed, "to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space." (Safire 2004)

The devastating events of September 11, 2001 changed how the world looked at security in general. Daily life routines have been altered permanently. Security for public and government infrastructures has never received such intense scrutiny as before. Governments worldwide are all eager to prevent such horrific incidents from ever happening again. Likewise, security in Cyberspace has also received significant attentions. In his letter to the United States citizens and as a foreword for *The National Strategy to Secure Cyberspace* (NSTSC 2003), President George Bush highlighted the importance of engaging and empowering Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. He mentioned that securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from the entire society, the federal government, state and local governments, the private sector, and the American people. The following are extracts from his letter:

The way business is transacted, government operates, and national defense is conducted have changed. These activities now rely on an interdependent network of information technology infrastructures called cyberspace. The National Strategy to Secure Cyberspace provides a framework for protecting this infrastructure that is essential to our economy, security, and way of life.

Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

The cornerstone of America's cyberspace security strategy is and will remain a public-private partnership. The federal government invites the creation of, and participation in, public-private partnerships to implement this strategy. Only by acting together can we build a more secure future in cyberspace. (NSTSC 2003)

The future of cyber security will be dependent on the cooperative effort and actions from individual organizations, vendors of computer systems, and policy makers.

B. COMPUTER SECURITY AWARENESS AND TRAINING

With the extensive use of computing resources in the running of their businesses or operations, most organizations are compelled to employ an Information Security Specialist or IT Manager in an effort to ensure business or operational continuity. Although these IT specialists are considered the frontline in the organization's defense of information security and risk management, it is sine quo non that achieving information security requires effort by all personnel in the organization. Just a single, untrained end-user is needed to defeat any well thought-out and well-executed security strategy adopted by the organization. All personnel must be aware of their responsibility and obligation to their organization's information security policies and procedures. Organization-wide awareness of information security can only be achieved by providing a constant and consistent information security educational program to all personnel.

The National Strategy to Secure Cyberspace NSTSC (2003) identified cyberspace security awareness and training programs as one of the five national priorities. The following extracts from NSTSC discussed the importance of end-user training to cyberspace security:

> Many information-system vulnerabilities exist because of a lack of cyberspace security awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers, chief executive officers, and corporate boards. These vulnerabilities can present serious risks to the infrastructures - even if they are not actually part of the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certifications for personnel further complicate the task of reducing vulnerabilities. The National Cyberspace Security Awareness and Training Program will raise cyber-security awareness in companies, government agencies, universities, and among the Nation's computer users. It will further address shortfalls in the numbers of trained and certified cyber-security personnel. (NSTSC 2003)

The problem with education and training in computer security is that it is often viewed as mundane and boring for both the users and administrators (Irvine 2003, 1). Computer security is an ever-evolving and complex topic, which the traditional

pedagogical ways of security education often fail to drive home in the intended lessons. Security seminars and formal classes describing security policies and technologies are usually not appropriate for the average end-users and are often beyond their grasps. IT managers' PowerPoint briefs on security awareness are often treated by end-users as boring and a waste of time and may not result in the appreciation of their obligations and responsibilities to be part of the overall security scheme.

The problem now is to find a security training tool that will interest the targeted audiences, and at the same time satisfy security training requirements. Will the solution to the above problem lie in the form of an interactive commercial-quality video game that has a security oriented theme? Would a security training tool that can be readily configured to simulate real world security issues be useful? Would a tool that can be scaled to train computer security personnel, from entry-level to experts, be helpful?

C. CYBERCIEGE AS AN IDEAL COMPUTER SECURITY EDUCATIONAL TOOL

As described in Irvine (2005, 2), effective information security requires both a practical and tacit understanding of the science and art of security engineering. Laboratory experiments can help convey these concepts, but a wide range of large-scale, realistic experiments would be too costly for most classrooms. Simulations thus provide a helpful alternative.

''CyberCIEGE is a high-end, commercial-quality video game developed jointly by Rivermind and the Naval Postgraduate School's Center for Information Systems Security Studies and Research. This dynamic, extensible game adheres to IA principles to help teach key concepts and practices'' (Irvine 2005, 2). It is a resource management simulation that attempts to model real-world security vulnerabilities. The game player is required to act and decide on IT related issues in a virtual IT-dependent organization. In order to meet the game objective, the player has to ensure the happiness and productivity of his virtual users in the organization while providing the necessary security measures to protect the organization's valuable and vulnerable information assets. The player's choices and decisions on procedural, technical, and physical security will determine

his/her success in achieving the game objectives. Figure 1 depicts a CyberCIEGE game play screenshot.
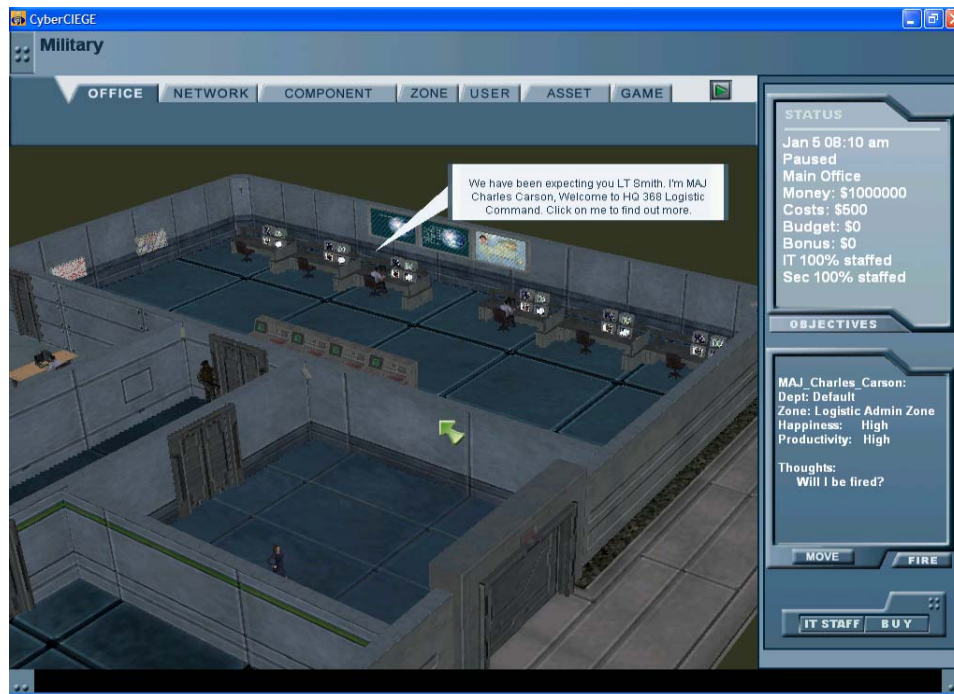
Figure 1.   CyberCIEGE game play screenshot

The main idea behind CyberCIEGE is that security concepts that are considered by some as mundane and boring can be taught in a more effective and entertaining manner. The following quotations highlight some advantages of using computer games as learning tools:

> Games are attractive because they challenge players, require the use of imagination, and satisfy the player's curiosity, thereby encouraging experiential and exploratory learning. The pedagogical advantages of games include their ability to motivate students and (they serve) as a vehicle for conveying a large body of information. (Kirriemuir 2002)

> In its latest effort, Microsoft is funding university projects that rewrite computer science curricula around something everyone knows students like: computer games. This year Microsoft awarded six universities a total of $480,000 to create new kinds of computer science courses in which students learn programming techniques using gaming software models. As part of the effort, teaching modules and entire courses will be offered free to the public in the company's Curriculum Repository… The goal has been to replace the earlier "drill-and-practice" methods of interactive learning with a new generation of pedagogical tools, for all educational levels and

11

in subjects ranging from science, mathematics, and engineering, to social sciences and humanities. (Angiolillo 2005)

CyberCIEGE consists of three main elements used for the construction of game scenarios. The following descriptions of the CyberCIEGE elements are derived from Irvine (2005, 2). The interested reader is encouraged to follow up with detailed readings.

1. Simulation Engine

This is a game engine that provides CyberCIEGE with an artificial intelligence system, video-playback library, library, memory-management system, resource-management, and real-time economic engine designed to support resource management simulations.

2. Scenario-Definition Language

This is a language used by CyberCIEGE scenario designers to express security-related risk management trade-offs, which the simulation engine will interpret and present as a simulation.

3. Scenario-Development Tool (SDT)

This is a development tool that elevates scenario designers from the complexity of the scenario language syntax during development of CyberCIEGE scenario. It supports reusable libraries of scenario elements and includes tools for compiling, validating, and running newly constructed scenarios as simulations (Johns 2004). Figure 2 shows a typical screenshot from the scenario-development tool.
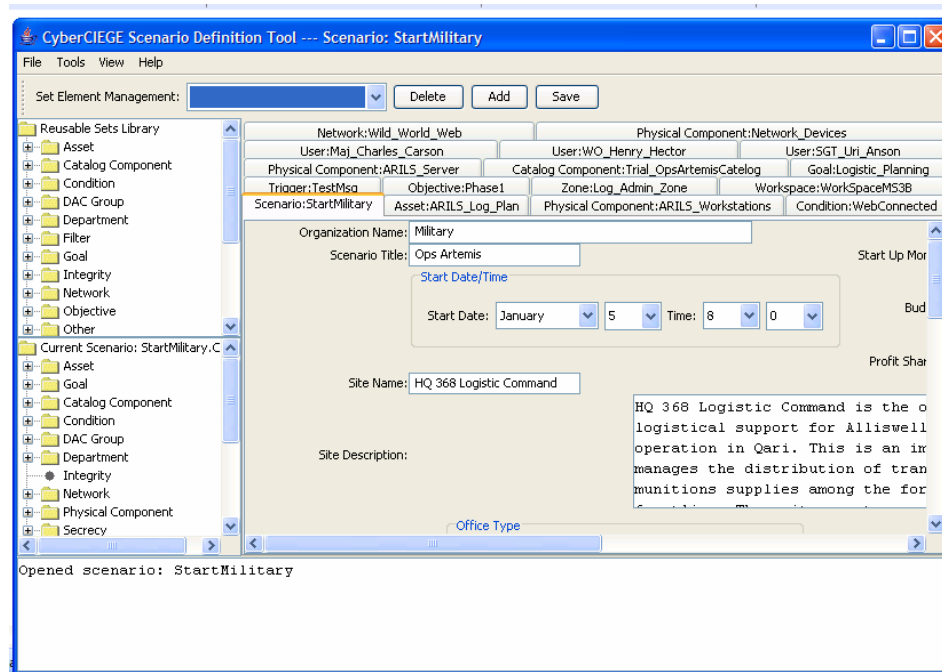
Figure 2.   Scenario-Development Tool

CyberCIEGE also comes with a video-enhanced encyclopedia covering a broad range of IA topics which the player can invoke anytime during game play to further his understanding of a particular security subject or a certain section of the game.

The application of simulations or games for the purposes of teaching security concepts does not need to be restricted to the academic arena; any organization that requires an interactive and stimulating tool to teach or reinforce security concepts will find CyberCIEGE a useful security educational tool that is both entertaining and captivating for the end-users.

D.   INTEGRITY OF MILITARY COMPUTERS

In today's heavily-wired world, attacks on military computer systems are becoming a growing threat to a nation's security. As mentioned in GAO (1996), at its simplest, these attacks would result in financial nuisance to the Defense department. At its worst, they can pose catastrophic threats to a nation's security. Critical computing resources for targeting systems, weapons system development, logistical and financial elements of the military are potential targets for attacks by adversaries.

When military computer systems are connected to the Internet, they become particularly susceptible to attacks. The exposure to the estimated 958 million (NetStat 2005) Internet users worldwide greatly increased the risks of unauthorized access to information and the potential disruption of critical services by malicious outsiders.

An article in *Federal Computer Week* reported that United States military computer networks are under constant attacks from its adversaries:

> Defense and industry officials describe DOD networks as the Achilles' heel of the powerful U.S. military. Securing military networks is even more critical in an increasingly transformed military in which information is as much a weapon as tanks and assault rifles. DOD networks have been breached. Department officials acknowledged hackers attacked military networks almost 300 times in 2003 — sometimes by cyber Trojan horses, which can operate within an organization's network. DOD officials say intrusions reduced the military's operational capabilities in 2004. The pace of the attacks has accelerated as adversaries honed in on this perceived weakness. DOD tallied almost 75,000 incidents on department networks last year, the most ever. (FCW 2005)

A year 2000 United States General Accounting Office (GAO) report highlighted that Federal Aviation Administration (FAA) was facing serious and pervasive problems in its agency-wide computer security program. The same report also reported a staggering increase in detected attacks on Defense Department networks and the need for federal government agencies to secure their critical computer system. The following are extracts:

> The fourth annual survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation (FBI) showed an increase in computer security intrusions for the third year in a row. In addition, the Defense Information Systems Agency recently reported that a total of 22,144 attacks were detected on Defense Department networks last year, up from 5,844 in 1998. Recognizing the federal government's increasing reliance on computer systems to perform its basic missions, it is imperative that agencies secure their critical computer systems and electronic data. (GAO 2000)

In its quest to safeguard its information systems, the military will face the same risks and challenges as any other government or private sector organization that has heavy reliance on computer and information technology. The ever-increasing sophistication and creativity of the attackers and their tools add on to the challenge of precluding unauthorized users from compromising the confidentiality, integrity, or

availability of information systems. A total cut off from external networks or an absolute protection of the military information systems is neither practical nor affordable. Risk management and tradeoffs that take into consideration the magnitude of the threat, the value and sensitivity of the information to be protected, and the cost of protecting it must be made when adopting computer security solutions.

The Battle of Tannenberg and the Battle of Midway, as discussed in an earlier section of the chapter, illustrated how the failure in ensuring secrecy of information can result in a dramatic change of fortunes for military forces. In both examples, the confidentiality of the military communication and information systems were compromised and these were key factors that shaped the outcome of both wars. Similarly, the loss of integrity in operation critical systems can also be disastrous as seen in the example of the "Farewell Dossier" campaign. The malicious software that was planted by adversaries triggered the destruction of the Trans-Siberian pipeline and led to the financial crippling of the Soviet Union.

The significance of maintaining secrecy in information systems compared to the importance of ensuring the systems' integrity had always been better illustrated in books and movies; hence, secrecy as a critical aspect in information assurance is better understood by the general readers. However, having both secrecy and integrity are of essence to achieving information assurance. This thesis focuses on illustrating the importance of maintaining the integrity of mission-critical systems in a military environment and will also highlight the consequences of compromising system integrity.

Information security is, without doubt, critical to mission success and can seriously impact a nation's security and survivability. With that understanding, we are left to question how nations and organizations are protecting their valuable computing resources and information assets.

The United States Navy recently implemented new policies to restrict service personnel's use of commercial, web-based email applications in an effort to mitigate the risk of attacks and to improve operation security. The following are quotations from DCMil (2005) that discussed the Navy's new policies:

The Navy has begun enforcing policies set forth in its Information Technology User Acknowledgement Form by blocking access to Web-based, commercial e-mail sites (webmail) from Department of the Navy-funded networks. That means it's no longer possible for anyone using Navy information technology to access commercial webmail from providers such as Yahoo, Hotmail, AOL, and others. (DCMil 2005)

"Navy Networks are a weapon system and must be defended with the same rigorous standards as other weapon systems," explained Vice Adm. James P. McArthur, commander, Naval Network Warfare Command (NETWARCOM). "People and mission are at risk without access to assured, secure, complete, accurate, and timely information." (DCMil 2005)

The restrictions on commercial webmail are necessary to protect the Navy's networks from multiple threats while maintaining operational security on all of its systems that are connected to the Department of Defense's Global Information Grid. (DCMil 2005)

To a certain extent, denying access to web-based email can improve the overall security of the network. The end-users are blocked from opening malicious email attachments that could potentially harm the organization's network. However, is that initiative enough to protect the network from the other multiple threats that exist on the Internet? How effective are the implementation of firewalls and gateways as cyber security solutions? Are firewalls and gateways strong enough to prevent intrusion into the organization's network when it is connected to the Internet?

It appears that the only infallible solution is to be completely shut out and disconnected from the Internet; however, this may not be practical as life today revolves so much around the Internet. A total disengagement from the Internet will result in a whole new set of issues. Is the solution to establish a network that is strictly reserved for Internet access only and completely separated from the organization's backbone network? Will an air-gapped network architecture as a security solution defend against a determined attacker? Even with an air-gapped network architecture, the commercial software or other potentially malicious software that is residing on the network can still pose serious security threats to the connected assets. The integrity of software and

hardware devices that are not developed under a controlled environment is susceptible to compromise by determined adversaries or professional hackers with a nation's resources at their disposal.

Software and hardware devices of uncertain origin are definitely potential threats to the integrity of military and government systems, which are high value targets to adversaries. The ever increasing reliance on commercial-off-the-shelf (COTS) technology operating on a broad array of military computer systems, which includes weapon systems, command and control systems, financial systems, personnel systems, payment systems, and other operational applications, is a cause of security concern. Although COTS technology does provide the advantages of lower development costs and access to frequent technology updates, its use will inevitably expose the defense software and systems to a great variety of local or even foreign suppliers and contractors. These greatly increase the risk of vulnerabilities exploitation and may cause serious security implications to a nation's defense setup. The following extracts from IT Pro (2005) and GAO (2004) highlight some advantages of COTS and the potential security threats they may pose:

> Economically, outsourcing creates several advantages and incentives for US corporations. First, they enjoy significantly reduced labor costs. Skilled labor in a developing market can be significantly cheaper than comparable US labor. Considering that outsourced labor usually does not receive healthcare or retirement benefits, the labor savings to US corporations can be even greater. Second, outsourcing provides a constant and reliable labor supply in the host country that is largely immune to local, regional, or even national labor supply spikes and dips that affect the outsourcing nation's labor market. Finally, outsourcing can create economies of scale that further drive down costs and save resources. (IT Pro 2005)

> Corporations must balance the benefits of outsourcing high-tech software development and application service provisioning against the costs, especially with regard to homeland security. (IT Pro 2005)

> DOD acquisition and software security policies do not fully address the risk of using foreign suppliers to develop weapon system software… other policies intended to mitigate information system vulnerabilities focus mostly on operational software security threats, such as external hacking

and unauthorized access to information systems, but not on insider threats, such as the insertion of malicious code by software developers. (GAO 2004)

As a System Administration Officer during a previous tour of duty in the Singapore Armed Forces (SAF), the author had the privilege of understanding and experiencing the challenges of managing a military unit's computer information systems and networks. SAF's choice of an air-gapped network for internal communications has the advantages of assuring secure information transfer between trusted systems and reducing vulnerabilities from outsider attacks; however, it also poses other interesting challenges such as the management of end-users' need for transferring data to and from an external source and end-users' desire to be connected to the host of services and resources available on the Internet.

A part of this thesis will be dedicated to investigating, from the perspective of information assurance, the use of commercial software on an air-gapped network versus connecting the network to the Internet. In both cases, the subjection of the network to possible malicious acts by adversaries will be explored. Motivated by the author's background, this thesis research aims to create a CyberCIEGE scenario that will mimic the real world challenges that a System Administration Officer in the Army will encounter while managing military information systems and networks. The scenario will focus primarily on the player maintaining the integrity of information system and networks in a military environment while supporting various end-users' needs. This thesis will contribute to the overall objective of the CyberCIEGE project, to create an alternative to traditional Information Assurance (IA) training and education approaches by developing an interactive, entertaining commercial-grade PC-based computer game that teaches IA concepts while simultaneously entertaining the player.

E.   KEY CONCEPTS AND DEFINITIONS

The following section provides definitions for key security concepts that are covered in this thesis. Understanding these key security concepts will allow readers to fully appreciate the security lessons brought forward by the CyberCIEGE scenario developed in this thesis. Unless stated otherwise, the majority of the definitions are

derived from the National Information Systems Security (INFOSEC) Glossary (NSTISSI 4009), published by the National Security Telecommunications and Information Systems Security Committee of the United States federal government to provide a common vocabulary for discussing INFOSEC.

1.   Information Assurance (IA)

Information operations (IO) that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (NSTISSI 4009)

2.   Computer Security

Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. (NSTISSI 4009)

3.   Information Systems Security (INFOSEC and/or ISS)

Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. (NSTISSI 4009)

4.   Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI 4009)

5.   Integrity

Quality of an information system (IS) reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (NSTISSI 4009)

6.   Availability

Timely, reliable access to data and information services for authorized users. (NSTISSI 4009)

7. Network System

System implemented with a collection of interconnected components. A network system is based on a coherent security architecture and design. (NSTISSI 4009)

8. Internet

A global network connecting millions of computers. More than 100 countries are linked into exchanges of data, news, and opinions. Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well. There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP). The Internet is not synonymous with World Wide Web. (Webopedia 2005)

9. Intranet

A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the *firewall* surrounding an intranet fends off unauthorized access. (Webopedia 2005)

10. Air-gapped Network

A network of interconnected components that implements both physical and logical separation from any other external network. Isolation is used to keep the flow of information within the interconnected components and reduce the risk of network vulnerability exploitation by outsiders. When the risks and consequences of attacks by adversaries are high, organizations such as government agencies and defense departments with interconnected systems that are sensitive or pertain to national security will often choose to adopt the air-gapped network architecture to isolate these systems from any other external networks such as the Internet.

F. SUMMARY

Securing information systems and networks is a complex and constantly evolving challenge. It requires the close collaboration of all concerned parties, from individual

end-users to policy makers, in order to have any chance of success. The importance of information security in military operations can never be overstated, and history has borne witness to numerous occasions where the success or failure of a campaign rested solely on the secured exchange of information. In this chapter, CyberCIEGE has also been depicted as a security training tool that can contribute to improving cyber security, and ultimately, may provide a more secure environment for information exchange. The background information and ideas provided in this chapter will act as guiding principles and motivations for the subsequent development of a CyberCIEGE scenario that will mimic the real world security issues in maintaining system integrity in a military environment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SCENARIO STRATEGY

This chapter discusses how CyberCIEGE can be used as a security educational tool to improve the security awareness level of personnel in an organization that has demanding needs for integrity of operational critical networks. The chapter will look at how CyberCIEGE can be used to teach security topics such as the importance of having physical security and the importance of software integrity for mission-critical systems in a military environment. This chapter also explores how CyberCIEGE can be used to simulate the tension between end-users' desire for Internet connections and the organization's need to protect its sensitive networks through its choice of an air-gapped, network architecture.

A. EDUCATIONAL FOCUS

As discussed in the Chapter II, just a single, untrained end-user is needed to compromise any well thought-out and well-executed security strategy adopted by an organization. In the context of a military environment, poor security awareness and training can be catastrophic. Therefore, having a security-educated workforce is vital for the military.

The following extracts from an article in *Federal Computer Week* indicated the United States DOD's budgeting concerns regarding IT and national security systems:

> DOD's fiscal 2006 budget contains $30.1 billion for IT and national security systems, according to GEIA's budget forecast. The defense IT budget will grow to $34.8 billion in fiscal 2011, but defense industry analysts at the conference warned that DOD plans to start few new projects in an environment defined by streamlining and consolidation… Defense vendors that succeed in the future will be those that offer innovative approaches to slow or stop increases in DOD's operations and maintenance costs… (FCW3 2005)

With tight budget controls, resources that can be allocated to IA security training efforts will also be limited. As such, CyberCIEGE is ideally positioned to provide an innovative yet cost effective means of IA security training to DOD personnel.

The flexibility of CyberCIEGE's game engine and scenario definition tool (SDT) will allow the creation of scenarios to meet a broad range of audiences and trainees. Scenarios may be custom-built to train and improve the IA security knowledge of policy makers, IT personnel, and end-users, thus raising the overall IA awareness level of organizations.

The CyberCIEGE scenario developed for this thesis will focus on illustrating the importance of maintaining the integrity of mission-critical systems in a military environment. The game scenario will also highlight the consequences that can result from compromising the integrity of these mission-critical systems. The sections to follow will describe how the tools and elements in CyberCIEGE can be used to build a scenario that covey these security concepts and lessons to players in a military environment.

B. SCENARIO STRUCTURED TO ACHIEVE EDUCATIONAL GOALS

The scenario was organized into a series of phases, each having one or more objectives that focus on a particular security educational goal. The following sections will describe the scenario design strategies used to illustrate and convey to the player the importance of maintaining physical security, hardware and software integrity for sensitive systems, and the need to maintain an air-gapped network architecture to protect a sensitive network.

C. USING CYBERCIEGE TO ILLUSTRATE THE IMPORTANCE OF MAINTAINING PHYSICAL SECURITY

Physical access into military facilities is usually controlled and monitored by guards and security personnel. The backgrounds of personnel working in these facilities are checked and they are considered trusted agents of the organization. Nevertheless, when access to operational systems with critical assets is not correctly restricted, there is still a possibility that the systems and assets will be unintentionally corrupted by 'trusted' insiders who are not proficiently trained. Therefore, adopting the right, physical security measures is fundamental to achieving information security.

Figure 3 illustrates a situation in which a workstation that holds critical assets on its local hard drive is placed in an area where there is little or no access control policies (i.e. an unsecured zone). With such an arrangement, it is inevitable that the workstation will be exposed to a variety of personnel with different clearance levels. This could subject the workstation and its mission-critical assets to possible corruption either by insiders who may have malicious intent or just through unintentional user negligence. The solution to this situation will be to move the workstation to an area with the right physical security measures and to enforce strict access control policies (i.e. a secured zone). This will minimize the exposure of the workstation and its critical assets to unauthorized personnel, thus reducing the risk of compromising the critical assets' integrity.

Physically secured area with strict access control policies	Area with less or no access control policies
	Workstation with critical assets on local hard drive
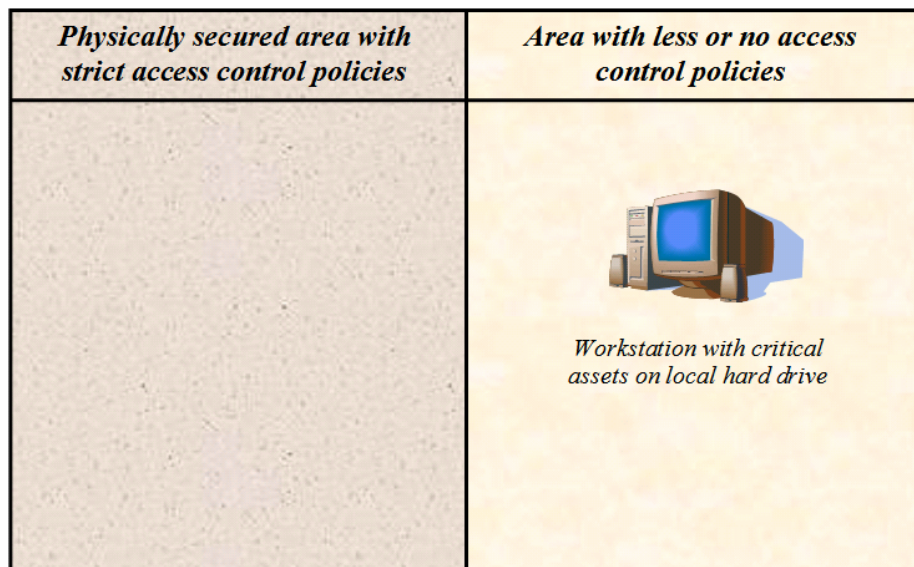
Figure 3.　　Situation One -Workstation in unsecured zone

In the second situation as shown in Figure 4, a workstation in an unsecured zone is assessing mission-critical assets that are held by a server in a secured zone. Although the mission-critical assets are now residing on a server in a secured zone, such an arrangement can still potentially expose the assets to possible corruption by unauthorized personnel that have physical access to the connected workstation in the unsecured zone. To solve this security problem, will it be enough to just move the workstation to the secured area?
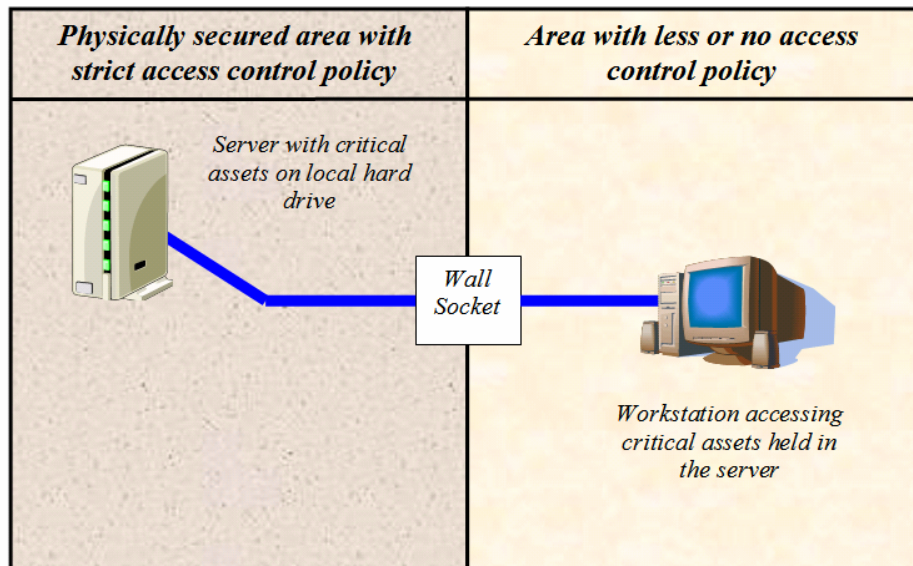
Figure 4.   Situation Two – Mission-critical assets on server

Figure 5 shows a proposed solution to the security problem illustrated in Figure 4; however, it seems as though this solution is not a foolproof one. The existence of the wall socket (i.e. CAT 5 or RJ-45 socket) could still be a potential vulnerability to the integrity of the mission-critical assets that are on the server in the secured zone. Unless this access point is physically removed or blocked, it can still be used by anyone in the unsecured zone for connecting another computer and gaining access to the server. Unauthorized personnel with malicious intent and motivations can potentially compromise the integrity of the mission-critical assets.
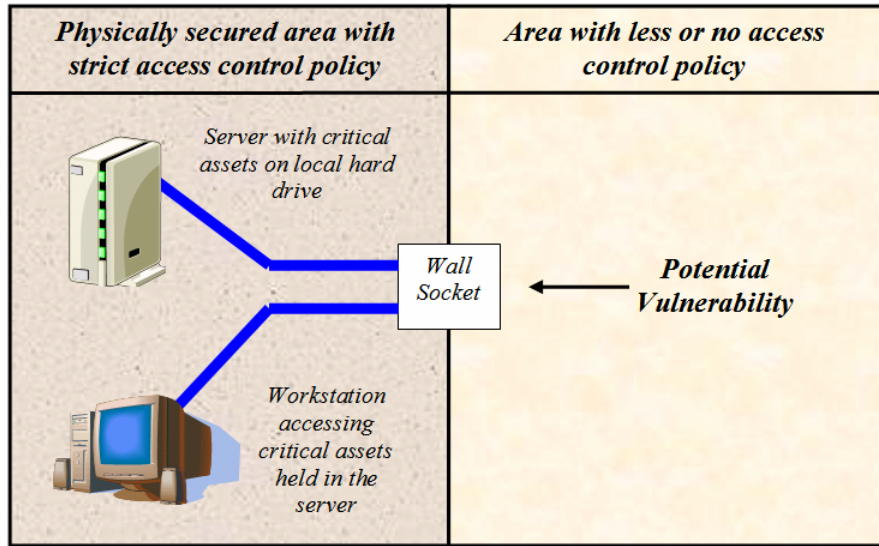
Figure 5.   Access point that could be a potential vulnerability.

A CyberCIEGE scenario can be built to portray the above situations and teach the player the importance of adopting the right physical security measures to protect the organization's mission-critical assets. The following section will describe the main CyberCIEGE components and elements that can be used to create a game scenario that will be able to mimic real life, physical security dilemmas and can be used to teach the player the appropriate security lessons.

A military logistics planning facility will be used as the backdrop for the scenario. The first phase of the scenario will start with the situation as illustrated in Figure 4. In this phase, the player will encounter a user who is in an area of the facility that is accessible to all personnel (i.e. an unsecured zone), working on a mission-critical asset, hosted by a server that is located in a secured zone with strict access control. To succeed in this phase, the player will have to provide the user with secured access to the server that is hosting the critical asset in order to protect this asset from being compromised. Secured access to the server can only be achieved via a LAN connection from a workstation that is also housed within the secured zone. To protect the integrity of the asset, the player will also need to ensure that there are no other network connections to the server from other workstations that are in the unsecured zone.

1. Scenario Briefings and Objectives

At the start of the CyberCIEGE game, the player is provided with a brief description of what is to be expected in the current scenario. Together with the objective description, scenario designers can indicate to the player what needs to be done to successfully complete the scenario. Message triggers can also be set to provide to the player hints and lessons learned if so desired.

In this scenario, the player will be told that he/she is the newly appointed IT manger of HQ 368 Logistic Command and his/her first objective is to ensure that all mission-critical assets in the facility are secured. Message triggers will also be used to trigger pop-ups that will show greeting messages and will introduce the key characters of the game to the player.

2. Zone

The CyberCIEGE game scenarios will consist of user accessible areas that can be partitioned into individual zones with different security attributes. The access to these zones can be controlled by setting the zone access list during game play or with the SDT. Similarly, physical security measures such as having a guard at the entrance to the zone, installing an expensive alarm, or having an iris scanner in the zone etc. can be set to reflect the different levels of physical security for the zones.

The scenario will consist of two main zones. For simplicity and clarity, the zone that is accessible by all users will be described as the unsecured zone, while the zone that has an access control list and is only accessible to users with a higher security clearance level will be known as the secured zone. The player will not be required to adjust the access lists or the enforcement mechanisms in the zones. The player cannot succeed by restricting access to the entire site because that will prevent one of the users, an administrative assistant with a lower security level, from accessing the zones and completing a future objective.

3. Asset

Assets, such as a mission-critical plan, can be created using the SDT and set to reside on workstations or servers in the game scenarios. The parameters of these assets, which include the costs resulting from the asset being attacked, the potential attackers, the attack motive level etc., can be set to reflect the different values or worth of the assets

to the organization and potential attackers. This will also result in different levels of attack motivation and will determine the levels of sophistication of the game engine attempts to compromise the assets.

To attract potentially, successful attacks, an asset with a high modification motive is defined. A Logistic Operation Plan is created as the mission-critical asset for this scenario. When the scenario starts, this asset will reside on a server within the secured zone and will be accessed by a user with a workstation that is in the unsecured zone. This setup can potentially expose the asset to users who do not have sufficiently high security clearances or who have low or no training; thus, resulting in the possible corruption of the asset. The player will have to learn this security lesson in order to succeed in this scenario; he/she will have to ensure that adequate physical security is accorded to this mission-critical asset.

4. User

Scenario designers can use the SDT to create users with different levels of trustworthiness and who will be assigned to work on goals.

A user in this game scenario will be given a goal that can only be satisfied by having access to the Logistics Operation Plan, a high integrity asset, as described in the previous section. The scenario will be designed such that the user will not have direct access to the server that hosts this asset; thus, the player will need to identify a zone that provides adequate physical security to house a workstation for securely accessing the asset via a LAN connection to the server. Most users in this game scenario will have clearances that include background checks to ensure the users' trustworthiness. At least one user will lack this clearance and background check. This user will have no authorized reason to access the Logistic Operation Plan, but because of low trustworthiness and low training level, this user may seek to compromise the asset. This user will also be given a specific motive to modify and corrupt the asset when it is exposed or becomes available in a zone that is accessible by him/her. The player may be able to increase the training level and trustworthiness of users by buying training and conducting background checks on them, respectively. To keep the player from changing

these aspects of the scenario, a budget constraint will be imposed. The limited fund available to the player will prevent him/her from buying training or getting background checks for any of the users.

5. Attack Triggers

Attack triggers provided by CyberCIEGE can be set to control the type and frequency of attacks on assets in the game. The game engine will also provide random attacks on the assets based on the motivation level of potential attackers.

The objective of this scenario is to convey security lessons on maintaining the integrity of military systems; thus, the attack triggers will seek to corrupt the assets rather than disclose them. Two main attack trigger types are used: one that triggers an insider's attempt to corrupt an asset and another that triggers malicious software to corrupt an asset.

6. Money

This can be used as a performance index to indicate how well the player is playing the scenario. It can be a reward for adopting the right security procedures in the game or as a penalty for failing to provide the right security measures in a given situation.

The player will start the game with limited funds so that unnecessary or undesired changes to the game aspects can be prevented – such as increasing trustworthiness and training levels of users.

D. COTS HARDWARE ISSUES IN A SENSITIVE ENVIRONMENT

As discussed in Chapter II, commercial-off-the-shelf (COTS) technology can be an attractive option in terms of cost effectiveness and the access to frequent technology updates. However, when such hardware devices, which may be of unknown origin, are deployed in a sensitive environment, the resulting consequences can be potentially catastrophic. A classic example is the "Farewell Dossier" campaign as discussed earlier.

CyberCIEGE does not specifically provide a function to set the integrity level of hardware devices in the game. Nevertheless, a combination of setting the platform, integrity level, and the type of software applications residing on the machines can be used to simulate the use of COTS technology and mimic the potential problem that can arise from their use.

As described in the previous section, to achieve the users' goals, the player must provide workstations for the users to work on their assigned tasks. In this phase of the scenario, the player must provide a second user access to the Logistics Operation Plan that is residing on the server. To achieve this objective, the player will need to purchase a workstation so that the second user can work on the asset in a secured zone. Four workstations with different attributes to portray different levels of hardware integrity will be made available from which the users may choose. To succeed, the player will need to buy the user a workstation that has the right integrity, house it in the secured zone, and connect it to the server via the LAN connection to access the asset.

1.   Components

Components in the CyberCIEGE game are used for storing and accessing assets by the users. Scenario designers can use the SDT to create a list of devices in the component catalogue to provide choices for the players when purchasing devices in the game's Buy Screen. These devices may be configured with a variety of OSs and base platforms that are of different integrity levels. A brief description of the devices in the Buy Screen of the game can also be included to guide or trick the player into making choices on his/her purchase. Devices that are configured with low integrity OSs or platforms will be more susceptible to attacks.

The player will be given a choice of four workstations in this scenario. The first is a lowly priced, basic workstation that is of a low integrity platform and installed with freeware. The second option is a high-end workstation with a low integrity platform that is bundled with both commercial software and freeware. The third option is an expensive workstation that has a trusted platform and was developed under a strict environment. The final option is a mid-priced, thin, client workstation that is on a trusted platform and without any software installed.

In the real world, an end-user's preference may, at times, sway the decision to acquire a particular system or device for the organization. In this scenario, message triggers that state the user's preference for the workstation will be added to entice the player into purchasing a workstation of the user's choice, which may not be the best

decision for a sensitive environment. To succeed, the player will have to select either of the last two described workstations, which have high integrity platforms that lack the extraneous, low integrity applications.

2. Attack Triggers

As described earlier, two main attack trigger types will be used in the scenario to trigger an insider's attempt to corrupt the asset and to trigger malicious software attacks on the asset. These attacks will succeed in corrupting the asset when the player makes a poor choice by purchasing a workstation of a low integrity platform with software applications of unknown origin installed and connects it to the server.

E. SOFTWARE INTEGRITY IN A SENSITIVE ENVIRONMENT

As mentioned previously COTS technology does have its advantages and disadvantages. Software that is of unknown origin has the potential to create havoc when installed on sensitive military systems. Commercial software products are usually just a fraction of the price of those that are developed under controlled environments. Often, they are also packed with richer features and may have better functionality, making them more appealing to the end-users. Therefore, when deciding on which software applications to acquire for use in a sensitive environment, factors such as cost, features available, end-users' preference, potential risks of sabotage etc. have to be weighed and taken into consideration before making the acquisition.

After the player has successfully deployed the high integrity workstation platforms in a physically secured zone and provided secure access to the Logistics Operational Plan for the user, the next phase of the scenario will introduce a need for a specific type of application that is developed within a secured environment. The player will need to acquire a logistics management software application in order to allow the users to meet their task objectives.

The player will be presented with three choices of logistics management software applications, each with a different set of security attributes and integrity level. The first option is a mid-priced, commercial logistics management software that is popular with the industry users and provides extensive features. The second option is a reasonably

priced, easy to use logistics software application that is highly favored by the military users. The third and final option is an expensive logistic management software that is developed under a controlled environment.

To complete this phase, the player will have to help the users accomplish their user goals by acquiring the high integrity, logistics management software. Purchasing the two software applications that are of lower integrity and installing them on the high integrity machines could potentially corrupt the mission-critical asset on the server. When deciding on the choice of software application to acquire, the player will have to weigh three key factors: the cost of the software application, user's preference, and sensitivity of the environment in which the application will be installed.

This phase of the scenario will demonstrate to the player that in order to achieve information security, it is also important to ensure the integrity of the software applications that are running on the systems.

1.   **Software**

CyberCIEGE has a set of predefined software products with different levels of integrity. Scenario designers can use the SDT to make these software products available for purchase by the player in the game. A brief description of these software products can be found in the CyberCIEGE encyclopedia which will provide the player with the required information for making his/her acquisition choices. Software products that are of low integrity can be potentially malicious and will increase the systems' susceptibility to attacks when installed.

As mentioned in the previous section, this scenario will introduce the need for the player to acquire a specific software application type that is of a high integrity level for use in a sensitive environment to satisfy the users' goals. Three different choices of the software application will be available for purchase by the player during the game. These software applications will be available in two forms: high integrity and low integrity. The descriptions of these software applications can be found in the CyberCIEGE encyclopedia and may be invoked by the player at anytime during the game play.

2. Message Triggers

As described earlier, message triggers can be set to trigger dialogue boxes which will illustrate the users' thoughts to the player during the game play. In this scenario, the message triggers will be used to invoke dialogue boxes that indicate the users' preference of software products. These messages from the users are aimed at influencing the player's decisions and will try to entice him/her to buy the software application that is preferred by the users - which may not be the right choice for the organization.

3. Money

There will be limited funds available to the player so as to mimic real life budget constraints that the player may encounter when purchasing software for the organization. The cost of the software applications will also be a factor that is used to influence the player's choice of software product to acquire.

F. AIR-GAPPED NETWORK ARCHITECTURE VERSUS NEED FOR INTERNET ACCESS

An air-gapped network architecture is a good way to reduce the organization's exposure from network vulnerabilities and a good way to protect its connected systems from outsider attacks. Implementing such network architecture will also mean forgoing connection to the Internet and access to valuable resources on the Web. This will likely create tension between end-users who desire access to the Internet and the organization's decision to disallow it. As discussed in the previous chapter, the solution could be to establish a network that is strictly reserved for Internet access only and completely separated from the organization's air-gapped backbone network.

With CyberCIEGE's rich set of functions and tools coupled with some imagination and creativeness from scenario designers, it is possible to develop a game scenario that can teach trainees security lessons based on the above described situation.

This last phase of the scenario will introduce the tension that is created when there is a need for users to be able to access the Internet while working in a sensitive environment. One of the users working in the secured zone and using a high integrity system platform and network will require access to an asset (i.e. Logistics Research Data) that can only be created with a connection to the Internet. Connecting the high integrity

systems and network to the Internet to create the Logistic Research Data will potentially expose the sensitive systems and network to malicious software and attackers, corrupting the mission-critical asset (i.e. Logistics Operation Plan) that is residing on the sensitive network.

To succeed in this phase, the player will have to help the user achieve the goal by creating a separate network that will be connected to the Internet. Another user will be tasked to work on the Logistics Research Data from a system that is connected to the Internet. Once the asset is created, it will be transferred onto the sensitive, air-gapped operation network via a dedicated system. This strict control of information transfer from the Internet to the sensitive network will help to ensure the integrity of the sensitive network.

1.   **Asset**

An asset, Logistics Research Data, will be created when a user is able to work on a workstation that is connected to the Internet. This asset will be subsequently transferred to the high sensitivity, air-gapped network via a dedicated system that is connected to the air-gapped network.

2.   **Networks**

CyberCIEGE provides the option for establishing multiple networks in the game. Scenario designers can use the SDT to create different networks for the scenarios.

This phase will require the player to form a separate network from the sensitive operational network in order to allow one of the users to access the Internet and create the Logistic Research Data.

3.   **Message Triggers**

At the start of this phase, one of the users working in the secured zone will want to connect to the Internet. This request is conveyed to the player through the dialogue boxes activated by the message triggers, portraying the users' thoughts.

4.   **Conditions**

CyberCIEGE provides the AssetToNetworkByFilterType condition which scenario designers can use to check for a network connection to a particular asset. In this scenario, when the player connects the sensitive network to the Internet for the first time,

this condition will trigger a warning message to warn the player of the danger of his action. A subsequent violation will set off the game-losing trigger (i.e. LoseTrigger).

G.   SUMMARY

This chapter has discussed how CyberCIEGE components and its game engine were explored to create game scenarios, mimicking real life information security issues, and used for conveying security lessons to a wide audience of trainees. The strategies for employing these CyberCIEGE elements to educate players on the importance of having physical security, hardware and software integrity, and how an air-gapped network architecture can enhance the security of operational critical systems in a military environment were also discussed in this chapter. The possibilities and variety of game scenarios that can be created are limited only by the game designers' imaginations. The next chapter will describe the results of using the strategies discussed in this chapter to implement a CyberCIEGE scenario that will illustrate the importance of maintaining systems integrity in a military environment.

IV. SCENARIO DESCRIPTION

As part of this thesis research, Operation Artemis, a CyberCIEGE scenario definition file (SDF), is developed to mimic real-world security issues encountered by military system administrators and to illustrate to players the importance of maintaining system integrity in a military environment. This chapter describes in detail the implementation of the scenario strategies as discussed in Chapter III. The objective is to create a SDF that can be used to convey security lessons about the need of having software integrity and an air-gapped network architecture in a sensitive military environment.

A. SCENARIO SETTINGS

This section will describe the CyberCIEGE game environment the players will encounter while playing the scenario.

The backdrop of the scenario is the army logistics command headquarters of the Republic of Alliswell, a fictitious nation. The player will be taking on the role of LT Norman P. Smith who was recently appointed IT manager of the logistics command headquarters, HQ 368 Logistics Command, Alliswell Armed Forces (AAF).

1. Initial Briefing

When the game is invoked, the following narratives will provide the context of the scenario and inform the player of his/her role in the game:

Welcome LT Norman P. Smith! We received your posting order and were expecting your arrival.

You are now the IT manger of HQ 368 Logistics Command. The security of the information systems and networks in the command is your responsibility.

We have heard good things about you from your previous command and we are expecting nothing less than your best here.

Proceed to the [Game] tab for a full briefing and instructions.

Good Luck Soldier!

2.   Full Description

When the player activates the 'Game' tab, he/she will be presented with a more in-depth description of scenario settings. The following are the narratives:

Good Day LT Norman P. Smith!

You have been appointed IT manager of HQ 368 Logistics Command, Alliswell Armed Forces (AAF).

The Republic of Alliswell is an island state 1° North of the equator in the Pacific. It has a population of 150 million and is one of the major economic powers in the world. The country has one of the best equipped and high-tech armed forces. Recent developments in the global war on terrorism has seen Alliswell deploying a huge number of troops in support of the allied forces' effort against insurgencies in the Middle Eastern state of Qari.

HQ 368 Logistics Command is the overall coordinator of logistical support efforts for AAF's operation in Qari. This is an important unit which manages the distribution of transportation, food and munitions supplies among the forces fighting in the frontline. The unit operates a sophisticated state of the art logistics management system from its home base, known as ARILS (AAF Real-time Integrated Logistics System). The system has real time links to the frontline troops and allows the monitoring and coordination of the forces' logistics assets. HQ 368 Logistics Command's operation is vital to the success of AAF's effort in Qari.

The game is organized into 5 phases Click on [Objectives] to see what they are.

Press "e" at any time to view the CyberCIEGE encyclopedia, which includes a "How To" section.

Press "k" to view the shortcut and navigation keys.

Click the "OFFICE" tab and then click on the red button (upper right) to begin play.

Good Luck Soldier!

3. Introduction of Users

At the start of the game, the player will be introduced to the four key characters in the scenario. SpeakTrigger is the trigger class used to invoke dialogue boxes that will provide a brief introduction and greeting messages to the player. The following are the messages:

Greetings from MAJ Charles Carson:

We have been expecting you LT Smith. I'm MAJ Charles Carson, Welcome to HQ 368 Logistics Command. Click on me to find out more.

Greetings from WO Henry Hector:

Welcome Sir! I'm WO Henry Hector, looking forward to working with you. Click on me to learn more.

Greetings from SGT Uri Anson:

Hi Sir! I'm SGT Uri Anson, I'm the IT assistant of the command. Click me to learn more.

Greetings from Ms Aida Young:

Hi Sir! Nice to meet you. I'm Aida, the new admin assistant. This is my first day on the job too!

B. ZONE LAYOUT

The scenario consists of six user-accessible areas that are partitioned into two main security zones, a secured zone and an unsecured zone, as described in Chapter III. The layout of HQ 368 Logistics command is shown in Figure 6.
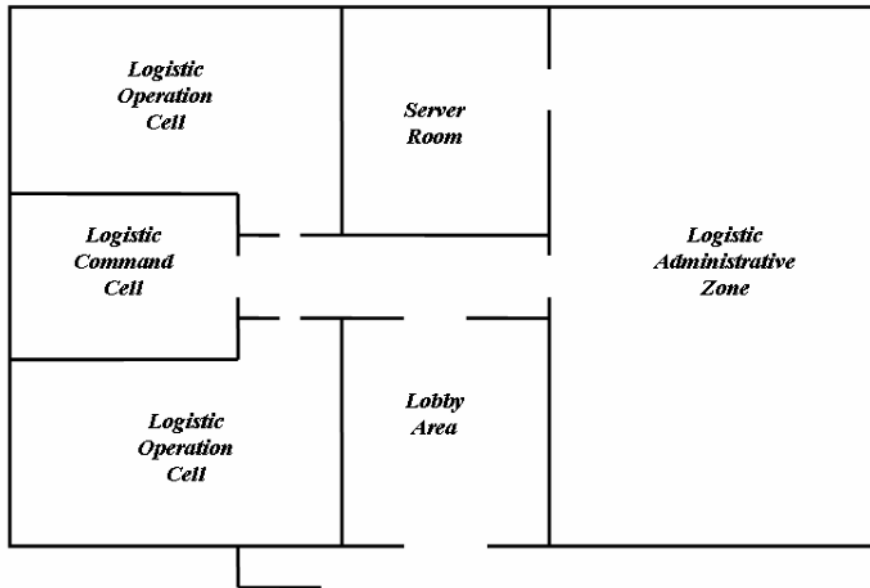
Figure 6.   Layout of HQ 368 Logistics Command.

Table 1 provides the descriptions of the different zones in the game scenario. It also shows the physical security attributes of each zone, users who are granted access to the zones, and the networks that are available in each zone. Players can click on the 'ZONE' tab in the game to view these zone attributes and descriptions.

Zone Name	Description	Permitted User	Physical Security Available	Network Available
Logistics Command Cell	This is the command cell of the Logistics operation, the nerve center of AAF's logistics operation.	MAJ Charles Carson	Guard at the door Prohibit Media Prohibit Phone Devices	ARILS IntraNet
Logistics Operation Cells	This zone is used for logistics planning and war gamming activities by the logisticians.	WO Henry Hector	Reinforced Walls Surveillance Cameras Expensive Alarm	ARILS Admin Net Lan Cable
Server Room	This room houses the server of HQ 368 Command. Mission-	SGT Uri Anson	Cipher Lock	

40

Zone Name	Description	Permitted User	Physical Security Available	Network Available
	critical assets are stored in the server.		Expensive Iris Scanner Key lock	
Logistics Admin Zone	This is the administrative area of HQ 368 Logistics Command. This zone is accessible by all personnel.	Public	Guard at the door Prohibit Media Patrolling Guard Reinforced Walls Moderate Alarm Key lock	ARILS Admin Net Lan Cable
Lobby Area	This is the lobby of HQ 368 Logistics Command.			

Table 1.   Scenario Zones Descriptions.

C.   USERS AND USER GOALS

As described earlier, there are four main characters in the scenario. These characters are assigned goals that they will try to meet in different phases of the game. The player's decisions during the game will affect and determine the ways these characters carry out their tasks. Their levels of success in achieving the assigned goals depends on the correctness of the player handling the given security situations.

Table 2 describes these four main characters and their assigned goals in the scenario. This information will be provided to the player when the 'USER' tab is invoked during the game.

Character Name	Description	Secrecy Level	User Goals
MAJ Charles Carson	Operation Commander of ARILS (AAF Real-time Integrated Logistics System) MAJ Carson is a no-nonsense commander who takes good care of his subordinates. This is his 12th year working in the AAF.	Secret	Phase 1: MajCarson_Work_on_LogPlan Phase 3: LogPlanners_Use_NewSW
WO Henry Hector	Assistant Operation Commander of ARILS. WO Hector is an able assistant to MAJ Carson and has 17 years of working experience in the AAF.	Secret	Phase 2: WoHector_Work_on_LogPlan Phase 3: LogPlanners_Use_NewSW
SGT Uri Anson	Assistant IT specialist of HQ 368 Logistics Command. SGT Anson assists the IT manger in managing IT issues in the command.	Secret	Phase 5: Secured_Data_Transfer

Character Name	Description	Secrecy Level	User Goals
	He is techno-savvy and enjoys working around computers and servers. He has 6 years of working experience in AAF.		
Ms Aida Young	Administrative Assistant to Operation Commander of ARILS. Ms Young is a newly hired civilian. She is a fresh graduate of Alliswell National University and this is her first job.	Restricted	Phase 4: Aida_Work_on_WebResearch

Table 2.   Scenario Characters and Goals Descriptions.

D.   COMPONENT CATALOG

The second phase of the scenario requires the player to purchase computer peripherals for WO Henry Hector. The devices available for acquisition will differ in terms of function, price, and integrity level. This will allow the player to experience the real-world dilemma of having to make the right acquisition choice in a given security situation while working with a limited budget. The choice of the purchase will reflect the player's appreciation of the security situation and lessons.

Table 3 provides the description of the devices available for purchase by the player. The component descriptions will be shown in the 'Buy' screen when the player clicks on the 'Buy' icon during the game.

Category	Descriptions	
PC	**Component Name**	Deal Basic
	Component Descriptions	Voted budget PC of the year by popular computer magazine, COMPView. This PC is bundled with a variety of freeware.
	Base Component	Lunitos AFOS
	Operating System	Populos V8 Desktop
	Software	URL2U Euphoria Word Triangle Placebo
	Cost	$1200
PC	**Component Name**	Deal Pro V
	Component Descriptions	The professional's choice! By popular PC brand Deal, this PC comes with excellent customer service support. A full suite of software is also bundled with this PC.
	Base Component	Blato Desktop Select
	Operating System	Populos V8 Desktop
	Software	URL2U Euphoria Word Triangle Placebo Internet Contemplator Cell Life WordSmyth
	Cost	$2200
PC	**Component Name**	Gell Mil
	Component Descriptions	Jointly developed by Alliswell Armed Forces and local defense contractors. Certified for military use.
	Base Component	Targo Worksaver
	Operating System	GIN
	Software	-

Category	Descriptions	
	Cost	$4500
PC	**Component Name**	Gell Cool
	Component Descriptions	Great looking workstation by a local company. No software is bundled with this PC.
	Base Component	The Thin Man
	Operating System	GIN
	Software	-
	Cost	$2000
Server	**Component Name**	MIB Green Warrior
	Component Descriptions	A server jointly developed by Alliswell Armed Forces and MIB, a local defense contractor. Certified for military use.
	Base Component	Green Shade Server
	Operating System	GIN
	Software	-
	Cost	$16500
External Devices	**Component Name**	Gell Cool
	Component Descriptions	This is a high performance router by ConNEX. Voted reader's choice in COMPView.
	Base Component	CP Router
	Operating System	FlipOS
	Software	-
	Cost	$2000

Table 3.   Component Attributes and Descriptions.

E.   SOFTWARE COMPONENTS

The player will be required to purchase a logistics supply chain management software application in the third phase of the game. The following sections will describe the three software products available for purchase. These descriptions are available to the player when he/she activates the CyberCIEGE encyclopedia.

The player has to make a choice between the following three logistics supply chain management software products:

1.   Agile 2005

Description: This is a mid-priced commercial logistics software package. It provides extensive logistics management functions and is very popular with industry users. The company that produces Agile 2005 has a reputable and trustworthy technical support team. It also has a website that provides constant updates for its products.

2.   SureRight Pro

Description: This is a reasonably priced and easy to use logistics software package. It provides functions that support military logistics planning processes and thus, is highly favored by military users. The company that produces SureRight Pro is a reputable local company and is listed on the local stock exchange.

3.   LogOn

Description: A logistics management software package that is developed under a strictly controlled environment for the military. To be able to fully exploit LogOn's rich logistics management features, users have to undergo a three weeks training package. Due to its stringent validation process, LogOn is one of the most expensive logistics software applications available.

F.   MANDATORY POLICIES

Table 4 describes the two classification levels, SECRET and RESTRICTED, used in the Operation Artemis scenario. One of these security classifications is assigned to all the users and assets in the scenario. The game engine will use these classifications as the basis for enforcement of the Mandatory Access Control (MAC) policy on the assets.

Secrecy Classification	Attributes and Descriptions	
SECRET	**Description**	Security clearance of Secret and beyond is a prerequisite for personnel working on the logistics plans for Ops Artemis, AAF's operations in Qari. The information or material of this classification requires a substantial degree of protection and the unauthorized disclosure could cause serious damage to the national security of Alliswell and seriously impair its operations
	Security Level	10
	Value to Organization	100000
	Value to Attacker (1-1000)	200
	Initial Background Checks	High
RESTRICTED	**Description**	All personnel working in HQ 368 Logistics Command are cleared to a minimum security level of Restricted. The information or material of this classification requires protection and the unauthorized disclosure of that information could be harmful to AAF's national security.
	Security Level	6
	Value to Organization	1000
	Value to Attacker (1-1000)	50
	Initial Background Checks	Low

Table 4. Secrecy Attributes and Descriptions.

G. ASSETS

The assets are the information or materials that are of a certain value to the organization. Users will access these assets as part of their user goals. The following sections provide descriptions of the assets in the Operation Artemis scenario.

1.   Ops_Artemis_Log_Plan

This is the logistics coordination plan for Operation Artemis, AAF's operation in Qari. It is critical to the success of AAR's mission. MAJ Carson and WO Hector are the only two users allowed access to this asset. MAJ Carson will be assigned to work on this asset in Phase 1 of the scenario and WO Hector will also be assigned to work on it in the second phase. The asset has a classification of SECRET. There are two sets of potential attackers assigned, Ms Aida Young and Public, that have a high attack motivation value of 501.

2.   Log_Web_Research_Data

The Internet provides a rich source of information on the latest and most innovative logistics management methodologies. AAF is constantly reviewing and upgrading the way its logistics operations are carried out. The research will aid in the effort to improve and optimize AAF's logistics management approaches. Ms Aida Young will be assigned to work on this asset in the fourth phase of the scenario. The asset has a classification of RESTRICTED and there is a low attack motivation for attackers to compromise it.

H.   USER GOALS

User Goals define the needs of users to gain access to the specified assets. The users' productivity and happiness levels are affected by their ability to accomplish the assigned goals. The following sections describe the User Goals defined in the Operation Artemis scenario.

1.   MajCarson_Work_on_LogPlan and WoHector_Work_on_LogPlan

This goal will require the user to create and maintain the Logistics Plan for Operation Artemis which is critical to the mission success of AAF's Operation in Qari. MAJ Carson will be assigned to work on this goal in the first phase of the scenario. In the second phase, the player will have to purchase a high integrity computer and place it in the secured zone for WO Hector to work on the same goal.

2.   LogPlanners_Use_NewSW

This goal will require the player to purchase a new logistics chain supply management software product in order for the users, MAJ Carson and WO Hector, to

accomplish their goals. The player will have to purchase LogOn which is the only software product that is of high integrity and is suitable for use in the highly sensitive environment.

3. Aida_Work_on_WebResearch

This goal in Phase 4 of the scenario requires the player to provide Internet access to Ms Aida Young in order for her to work on the asset, Log_Web_Research_Data, and to accomplish this assigned goal. The player will have to ensure that he continues to maintain the air-gapped network architecture of the ARILS IntraNet while trying to provide Internet access for Ms Young. Connecting ARILS IntraNet to the Internet will corrupt mission-critical assets that are residing on the server.

4. Secured_Data_Transfer

This goal will be assigned to SGT Anson in Phase 5. The player will have to ensure that SGT Anson's computer in the server room is the only computer that has access to media devices. This can be done by setting the server room's physical security attributes to allow media access. The other zones in the scenario should have the Prohibit Media attribute set.

I PHASES AND OBJECTIVES

This section provides a description of the five game phases and the phase objectives created in the Operation Artemis scenario. The triggering conditions that will result in the completion or non-completion of the objectives in the phases are shown in Table 5.

1. Phase0_MoveAsset

This is the first phase of the scenario. It requires the player to identify the potentially unsecured setup in HQ 368 Logistics Command that may compromise the mission-critical asset residing on the ARILS server. To complete the scenario, the player will have to identify the Logistics Operation Cell as the safest and most secured zone in the building and set up the workstation that is in the zone, connecting it to the ARILS IntraNet in order for MAJ Carson to be able to work on the Qari_Log_Plan. At the same time, the player has to ensure that the ARILS IntraNet is not connected to the Internet or any other networks that are of lower integrity.

Although HQ 368 is a relatively secured building, there is still a need to ensure all mission critical assets are accorded the right amount of protection. The integrity of the assets may be compromised by accidental changes made by unauthorized or untrained personnel, or by determined adversaries who may attempt to corrupt or steal these assets.

Phase Description (i.e. Completed Text)

Well done Lieutenant! It is important to provide adequate physical security to protect the mission-critical assets from both accidental and deliberate corruptions.

2. Phase1_BuyPC

This is the second phase of the scenario. It requires the player to purchase a workstation that is built on a high integrity platform and place it in the secured zone, Logistics Operation Cell, for WO Hector to be able to work on the Qari_Log_Plan. The player will have to decide on one of the five available workstations in the component catalog. In order to achieve the objective, the player will have to buy either Gell Mil or Gell Cool workstation, which has a high integrity operating system and does not come installed with potentially malicious software applications.

Objective Description (i.e. Uncompleted Text)

WO Hector needs to assist MAJ Carson in working out the Qari logistics plan. In order for WO Hector to work on the plan and meet his goal, you need to provide him with a system and help connect him to the ARILS IntraNet.

Phase Description (i.e. Completed Text)

Acquiring high integrity systems from a trusted source is a critical part in maintaining IA for a sensitive environment. Unneeded software applications that are from unknown or non-trusted origin should not reside on high integrity systems, as they could potentially be malicious. Thus, not having them will help reduce the risk of compromising sensitive systems and networks. Good Job.

3. Phase2_BuySW

This is the third phase of the scenario. It requires the player to purchase a logistics supply chain management software application for the logistics planners, MAJ Carson and WO Hector. There are three logistics applications available for purchase and the player can invoke the CyberCIEGE encyclopedia to view their descriptions. To succeed in this phase, the player has to purchase LogOn, which is a logistics software application developed in a controlled environment for military use.

Objective Description (i.e. Uncompleted Text)

The command is looking for good logistics supply chain management software application that can aid the logistics planners in their work. Your task is to identify and purchase a suitable logistics management application for the command. You can find the descriptions of the available logistics applications in the CyberCIEGE encyclopedia. (Press 'e' to invoke CyberCIEGE encyclopedia.)

Phase Description (i.e. Completed Text)

It is important to ensure that software applications running on a sensitive network are of trusted origin. Software products with low integrity can potentially corrupt the network and its high integrity systems. Keep up the good work Lieutenant!

4. Phase3_ WebAccess

This is the fourth phase of the scenario. It requires the player to provide Internet access to Ms Aida Young so that she can accomplish her goal on researching logistics data on the Internet. In order for the player to complete this phase, he/she will have to provide an Internet connection for Ms Young and also ensure that the highly sensitive ARILS IntraNet and the mission-critical asset on it are not exposed to the Internet. ARILS IntraNet has to maintain the air-gapped network structure, so a separate network for only Internet access will have to be created.

Objective Description (i.e. Uncompleted Text)

The Internet provides a rich source of information on the latest and most innovative logistics management methodologies. AAF is constantly reviewing and upgrading the way its logistics operations are carried out. Ms Aida Young has been

tasked to research and work on the Log_Web_Research_Data. The research will aid in the effort to improve and optimize AAF's logistics management approaches.

Phase Description (i.e. Completed Text)

In order to satisfy the users' desire to connect to Internet in this sensitive environment, there is a need to maintain a network that is strictly for Internet access only and totally separated from the air-gapped backbone network. Well done Lieutenant!

5. Phase4_CntDataMvt

This is the fifth and final phase of the scenario. The users in the command requested that they be allowed to transfer data to and from the sensitive ARILS IntraNet, so the player will have to identify a secure way of satisfying this request. To complete this phase of the game, the player will have to ensure that the only zone in the building that allows media access is the Server room and the only computer that allows removable media is the one that resides in the server room. These will simulate and mimic the transfer of data through a trusted and controlled point.

Objective Description (i.e. Uncompleted Text)

The logistics planners requested that some of Ms Young's' web research data be made available to them. They also feel that it would be useful if they are able to move data between the networks. SGT Anson is looking for ways to meet these requests. Your task is to help SGT Anson determine the most appropriate way to perform the data transfer.

Phase Description (i.e. Completed Text)

It is important to prohibit or restrict media devices on sensitive systems in order to protect their integrity. A strict control on data movement between systems or networks with different integrity and sensitive levels is critical in protecting the high integrity systems or networks. Therefore, restricting the number of accessible avenues into the secure network is highly desirable. Great Job Lieutenant!

Phase	Objective	Objective Completion Status	Triggering Conditions
0	Obj_Phase_1ST_MoveAsset	True	MajCarson_Work_on_LogPlan **AND_NOT** AdminNet_To_LogPlan
		False	**NOT** MajCarson_Work_on_LogPlan **OR** AdminNet_To_LogPlan
1	Obj_Phase_2nd_BuyPC	True	Obj_ 1st_MoveAsset_Met **AND** WoHector_Work_on_LogPlan
		False	**NOT** Obj_ 1st_MoveAsset_Met **OR_NOT** WoHector_Work_on_LogPlan
2	Obj_Phase_3nd_BuySW	True	Obj_2nd_BuyPC_Met **AND** LogPlanners_Use_NewSW
		False	**NOT** Obj_2nd_BuyPC_Met **OR_NOT** LogPlanners_Use_NewSW
3	Obj_Phase_4th_WebAccess	True	Obj_3rd_BuySW_Met **AND** Aida_Work_on_WebResearch
		False	**NOT** Obj_3rd_BuySW_Met **OR_NOT** Aida_Work_on_WebResearch
4	Obj_Phase_5th_CntDataMvt	True	Obj_4th_WebAccess _Met **AND** Secured_Data_Transfer
		False	**NOT** Obj_ 4th_WebAccess_Met **OR_NOT** Secured_Data_Transfer

Table 5.   Phase and Objective Requirements.

J.   TRIGGERS

The following describes the main triggers defined in the Operation Artemis scenario.

1.   **User_Greetings**

The triggers, MajCC_Greetings, WoHH_Greetings etc, in this trigger group are of the trigger class, SpeakTrigger. They are used to activate dialogue boxes for introducing the users to the player.

2.   **Msg_To_Player**

These groups of triggers, Log_Plan_Attack_8_1st_Msg, Log_Plan_Attack_17_1st_Msg etc, are of the trigger class, MessageTrigger. They are used to activate text boxes during the game to inform the players of events that are happening.

3.   **Attack_Trigger**

There are two triggers in this group, Mal_Attack and Insider_Attack, both are of trigger class AttackTrigger.

Mal_Attack

This trigger will set off Attack Type 8. It has a set frequency of 0.05 which will cause the game engine to generate malicious software attacks on any exposed assets every three minutes.

Insider_Attack

This trigger will set off Attack Type 17. It has a set frequency of 0.05 which will cause the game engine to generate insider attacks every three minutes on any assets that are exposed to the public, or to users who do not meet the assets' MAC policy.

4.   **SetNext_Phase**

The triggers, 1st_Phase_Done_Next, 2nd_Phase_Done_Next, 3rd_Phase_Done_Next, 4th_Phase_Done_Next, are SetPhase triggers used for progressing to the next phase of the game when the player has met all the objectives of the phase.

5.   **Set_Objective_Status**

The triggers that are in this group include, Move_Asset_Done, BuyPC_Done, BuySW_Done, WebAccess_Done and CntDataMvt_Done. They are of trigger class, SetPhaseObjective and are used for indicating that a particular objective of the phase is completed when all the firing conditions of the triggers are met.

K.   CONDITIONS

The following describes the main conditions that are defined in the Operation Artemis scenario. The conditions are set in the scenario to check for the occurrences of a particular event which the game engine will use for executing the corresponding triggers.

1.   Timing

This group of conditions which include delay1hr, delay2hrs etc. are of condition class TimingCondition and are used for timing events in the scenario.

2.   Asset_Attacked

There are two conditions in this group, Malware_Atk_LogPlan and Insider_Atk_LogPlan. These are conditions belong to AssetAttacked condition class and are used for checking the occurrence of an attack on an asset

MalWare_Atk_LogPlan

This condition will check for the occurrence of an attack on the mission-critical asset, Ops_Artemis_Log_Plan, by malicious software.

Insider_Atk_LogPlan

This condition will check for the occurrence of an attack on the mission-critical asset, Ops_Artemis_Log_Plan, by an insider.

3.   LogPlan_In_OpsRm

This condition will check for the presence of Ops_Artemis_Log_Plan in the Logistics Operation Cell.

4.   Checking_Conditions

This group of conditions which includes AdminNet_to_LogPlan, Web_to_LogPlan, etc., is used to check for the occurrence of specific events in the game.

AdminNet_To_LogPlan

This condition will check if the mission-critical asset, Ops_Artemis_Log_Plan is found on the Administrative Network, ARILS Admin Net. Having the asset on the Admin Net is not desired as it will expose the asset to attacks.

<u>WebConnected</u>

This condition will check if the mission-critical asset, Ops_Artemis_Log_Plan is connected to the Internet. It is not desirable for the asset to be exposed to the Internet which will compromise it.

5.   Phase_Completed

This group consists of the five conditions 1st_Phase_Done, 2nd_Phase_Done, 3rd_Phase_Done, 4th_Phase_Done and 5th_Phase_Done. These are PhaseCompleted conditions and are used for indicating the completion of the phases.

6.   Objective_Completed

This group consists of the five conditions Obj_1st_MoveAsset_Met, Obj_2nd_BuyPC_Met, Obj_3rd_BuySW_Met, Obj_4th_WebAccess_Met and Obj_5th_CntDataMvt_Met. These are ObjectiveCompleted conditions and are used for indicating that a particular objective of the phases is met.

7.   Asset_Goal_Met

This group consists of the five conditions MajCarson_Work_on_LogPlan, WoHector_Work_on_LogPlan, LogPlanners_Use_NewSW, Aida_Work_on_Web and Research Secured_Data_Transfer. These are AllAssetGoalsMeet conditions and are used for indicating that a particular user goal has been achieved.

L.   SUMMARY

The virtual users, user goals, assets, components, devices, triggers, conditions etc. that were used to create the Operation Artemis scenario were discussed in detail in this chapter. Each of these elements contributes to the creation of a scenario that is capable of mimicking real world security issues found in a military environment and can be used to convey security lessons on the importance of integrity to players.

The next chapter will look at the testing done for this thesis. The objectives and methodologies used in the construction of Operation Artemis scenario test cases, and the test results will be discussed. The proposed solution to the scenario will also be provided.

V. SCENARIO TESTING

This chapter discusses the test objectives and methodologies applied to evaluate the execution of the Operation Artemis scenario. The two categories of test cases developed to evaluate the scenario are described in detail. This chapter also covers the informal testing conducted during the scenario development process which contributed to the improvement of the SDT and the CyberCIEGE game engine.

A. TEST OBJECTIVE

The purpose of conducting the tests was to demonstrate that the Operation Artemis scenario can reasonably simulate real-world behaviors and security issues found in a military environment.

The results from the tests and the bug fixes on the SDT and CyberCIEGE game engine contribute to the overall improvement of CyberCIEGE as a security educational tool and reduced unwanted non-deterministic aspects of the game engine.

B. TESTING METHODOLOGY

The approach taken to test the correctness of Operation Artemis involved the development of two categories of test cases. The first category identifies the desired or preferred game moves and the expected results from the execution of these moves. The second category of test cases identified several possible incorrect game moves that players could execute and the expected results from the execution of these moves.

C. TEST CASES

The following section describes the test objectives of the five phases in the Operation Artemis scenario and the two categories of test cases developed to evaluate the scenario. Table 6 shows the preferred game moves to achieve the scenario objectives and the expected results from the execution of these moves in the scenario while Table 7 shows the incorrect game moves that a player could possibly execute and the expected results from making such moves.

1.   **Phase 0 Test Objectives**

The test cases created for the first phase of the scenario are used to determine whether the phase was correctly developed to illustrate to the player the importance of maintaining physical security in a sensitive military environment.

2.   **Phase 1 Test Objectives**

For the second phase, the test cases evaluate if the phase was correctly developed to illustrate to the player that acquiring high integrity systems from a trusted source is critical to achieving IA in a sensitive environment. The test cases also check whether the phase can correctly illustrate to the player that unnecessary software applications from unknown or non-trusted origin should not reside on high integrity systems, as they could be potentially malicious.

3.   **Phase 2 Test Objectives**

The test cases for the third phase evaluate if the phase was correctly developed to illustrate to the player that for sensitive systems and networks, it is important to acquire only high integrity software applications developed within a trusted and controlled environment..

4.   **Phase 3 Test Objectives**

The test cases for this phase evaluate if the phase was correctly developed to illustrate to the player that there is a need to maintain an air-gapped network architecture for sensitive backbone networks of the organization.

5.   **Phase 4 Test Objectives**

This set of test cases for the final phase are used to evaluate if the phase was correctly developed to illustrate the importance of prohibiting or restricting removable media devices (e.g. USB ports, portable storage devices etc.) on sensitive systems when protection of system integrity is needed. Strict control of data movement between systems or networks with different integrity and sensitivity levels is critical in protecting high integrity systems or networks.

Phase	Test Case ID	Preferred Game Moves	Expected Results
0	TCA_P0	**Step 1**: The player removes the network connection between the ARILS_AdminNet and the ARILS_Server. **Step 2**: ARILS_PC4 is then connected to the ARILS_IntraNet which is also connected to the ARILS_Server. **Step 3:** MAJ Carson is assigned to work on ARILS_PC4 in the Logistics Command Cell. ARILS_PC4, which is connected to the ARILS_IntraNet, will be used for accessing the mission-critical asset, Ops_Artemis_Log_Plan.	The ARILS_AdminNet is disconnected from the ARILS_Server and cannot access the Ops_Artemis_Log_Plan. Thus, protecting the asset from malicious users. MAJ Carson has the "no asset goal" failure and is working on the Ops Artemis log plan in the operation logistic cell. The first phase of the scenario is completed. Proceed to the next phase.
1	TCA_P1	**Step 1**: In the 'Buy' Screen, the player purchases either the Gell Mil or Gell Cool workstation **Step 3:** The purchased workstation is placed on the empty table in the Logistic Command Cell and connected it to the ARILS_IntraNet and the ARILS_Server. **Step 4:** WO Hector is assigned to work in the Logistic Command Cell using the new workstation which is connected to the ARILS_IntraNet and can be used for accessing the mission-critical asset, Ops_Artemis_Log_Plan.	A new workstation of either the Gell Mil or Gell Cool model is purchased and placed in the Logistic Command Cell. WO Hector has the "no asset goal" failure and is working on Ops Artemis log plan in the operation logistic cell. Second phase of the scenario is completed. . Proceed to the next phase.
2	TCA_P2	**Step 1**: The player purchases the logistic management software application, Log On for the ARILS_Server that is in the Server Room.	A new logistic management software application is purchased and installed onto the ARILS_Server. Both MAJ Carson and WO Hector have the "no asset goal" failure and are working

Phase	Test Case ID	Preferred Game Moves	Expected Results
			on Ops Artemis log plan in the operation logistic cell. Third phase of the scenario is completed. Proceed to the next phase.
3	TCA_P3	**Step 1**: On the 'Network' screen, the player selects ARILS_Router3 which is located in the Logistic Admin zone and connects it to the Wild_World_Web to gain Internet access. **Step 3:** The ARILS_AdminNet icon is then connected to ARILS_Router3. **Step 4:** The player then assigns Ms Aida Young to either ARILS_PC1 or ARILS_PC2 in order for her to work on the Log_Web_Research_Data asset.	ARILS_AdminNet is connected to the Wild_World_Web. Both ARILS_PC1 and ARILS_PC2 which is on the ARILS_AdminNet can be used for accessing the Internet. Ms Young has the "no asset goal" failure and is using either ARILS_PC1 or ARILS_PC2 to work on the Log_Web_Research_Data. The fourth phase of the scenario is completed. Proceed to the next phase.
4	TCA_P4	**Step 1**: In the 'Zone' screen, the player selects the Server Room and unchecks the 'Block Removable Media' attribute of the 'Component Settings' panel. **Step 2:** On the 'Component' screen, ARILS_PC3 is selected and its 'Block Removable Media' attribute in the 'Default Configuration Settings' is unchecked.	Server Room is the only zone that allows removal media. ARLS_PC3 residing in the Server Room is the only workstation that allows removal media. SGT Anson has the "no asset goal" failure. The fifth phase of the scenario is completed. Scenario ended, player has

Phase	Test Case ID	Preferred Game Moves	Expected Results
			completed all the objectives in the Operation Artemis scenario.

Table 6. Test Case for Preferred Game Moves.

Phase	Test Case ID	Possible Incorrect Game Moves	Expected Results
0	TCB_P0a	**Step 1:** The player connects ARILS_PC4 which is in the secured zone, Logistic Operation Cell, to the ARILS_IntraNet and ARILS_Server and assigns MAJ Carson to ARILS_PC4. **Step 2:** ARILS_AdminNet is not disconnected from the ARILS_Server.	Even though MAJ Carson is working on the mission-critical asset, Ops_Artemis_Log_Plan, using a high integrity workstation in a secured zone, the player's failure in disconnecting the ARILS_AdminNet from the ARILS_Server will provide potential avenues of attack for malicious software and insiders to compromise the asset. Malicious software and insider attacks continue to compromise Ops_Artemis_Log_Plan. The phase objective is not achieved.
	TCB_P0b	**Step 1:** The player disconnects the ARILS_AdminNet from the ARILS_Server. **Step 2:** The player connects ARILS_PC4 which is in the secured zone, Logistic Operation Cell, to the ARILS_IntraNet and ARILS_Server and assigns MAJ Carson to ARILS_PC4 **Step 1:** The player connects	Disconnecting the ARILS_AdminNet from the ARILS_Server prevents unauthorized insider from compromising the asset. However, connecting the ARILS_IntraNet to the Internet will expose the asset to malicious attackers. Ops_Artemis_Log_Plan

Phase	Test Case ID	Possible Incorrect Game Moves	Expected Results
		ARILS_IntraNet to the Wild_World_Web using any of the routers available.	continues to be corrupted by malicious users on the Internet. The phase objective is not achieved.
1	TCB_P1a	**Step 1:** The player purchases a workstation that is neither of the two available high integrity models, Gell Mil and Gell Cool, that comes with a trusted OS and are on a higher integrity platform. **Step 2:** The player places the low integrity workstation in the secured zone and connects it to the ARILS_IntraNet and ARILS_Server and assigns WO Hector to it	Even though the WO Hector is working on the mission-critical asset in the secured zone. The low integrity platform of the workstation coupled with the unnecessary software applications of unknown origin, residing on the workstation, will compromise the asset. Malicious software attacks will compromise Ops_Artemis_Log_Plan. The phase objective is not achieved.
	TCB_P1b	**Step 1:** The player purchases a high integrity model workstation, Gell Mil or Gell Cool that comes with a trusted OS and is on a high integrity platform. **Step 2:** The player places the high integrity workstation in the unsecured zone and connects it to the ARILS_IntraNet and ARILS_Server and assigns WO Hector to it.	Even though the WO Hector is working on the mission-critical asset the zone that he is working in is unsecured. Thus, unauthorized insiders can potentially compromise the mission-critical asset. Insider attacks will compromise Ops_Artemis_Log_Plan. The phase objective is not achieved.
2	TCB_P2a	**Step 1:** The player purchases a logistics management software application that is not Log On.	Software applications that are of unknown origin or are not developed under a controlled environment have the

Phase	Test Case ID	Possible Incorrect Game Moves	Expected Results
		Step 2: The software is installed in any of the workstations or the server on ARILS_IntraNet.	potential to compromise the sensitive network and asset. Malicious software attacks will compromise Ops_Artemis_Log_Plan. The phase objective is not achieved.
	TCB_P2b	**Step 1:** The player purchases the logistic management software application, Log On that was developed under a controlled environment for military use. **Step 2:** Log On was installed in any of the network devices other that the ARILS_Server.	Not installing Log On on ARILS_Server will prevent anyone from gaining access to the application and the users will fail to meet their goals. Depending on where Log On is installed, either MAJ Carson, WO Hector or both logistic planners will have asset goal failures. The phase objective is not achieved.
3	TCB_P3a	**Step 1:** The player connects ARILS_AdminNet to the Wild_World_Web to gain access to the Internet. **Step 2:** Ms Aida Young is assigned to either ARILS_PC1 or ARILS_PC2 in the Administrative zone to work on the Log_Web_Research_Data **Step 3:** The player connects ARILS_AdminNet to the ARILS_Server.	Connecting the ARILS_IntraNet to the Internet will expose the asset to malicious attackers. Ops_Artemis_Log_Plan is corrupted by malicious users on the Internet. The phase objective is not achieved.
4	TCB_P4a	**Step 1:** The player unchecks the 'Block Removable Media' option of any zones other than the Server	SGT Uri Anson is in the Server Room with his workstation to provide a

Phase	Test Case ID	Possible Incorrect Game Moves	Expected Results
		Room to allow removable media devices in the specified zone.	centralized, trusted and controlled point for the movement of data between networks of different integrity levels. Allowing removable media in zones other that the Server Room will contradict the above policy. SGT Anson will have asset goal failure. The phase objective is not achieved.
	TCB_P4b	**Step 1:** The player unchecks the 'Block Removable Media' option of any workstations other than ARILS_PC3 that is in the Server Room to allow removable media devices on that specified workstation.	As mentioned earlier, the command's policy is to have a centralized, trusted and controlled point for the movement of data between networks of different integrity levels. Allowing removable media on non-authorized workstations will contradict the above policy. SGT Anson will have asset goal failure. The phase objective is not achieved.

Table 7.   Test Case for Incorrect Game Moves

D.   EVALUATION RESULTS

Table 8 summarizes the results of executing all the test cases that were described in Table 6 and Table 7.

Test No.	Test Case ID	Results
1	TCA_P0	As anticipated
2	TCA_P1	As anticipated
3	TCA_P2	As anticipated
4	TCA_P3	As anticipated
5	TCA_P4	As anticipated
6	TCB_P0a	As anticipated
7	TCB_P0b	As anticipated
8	TCB_P1a	As anticipated
9	TCB_P1b	As anticipated
10	TCB_P2a	As anticipated
11	TCB_P2b	As anticipated
12	TCB_P3a	As anticipated
13	TCB_P4a	As anticipated
14	TCB_P4b	As anticipated

Table 8. Scenario Evaluation Results.

E. INFORMAL TESTS

During the scenario development process, small sets of test cases were informally developed and used for evaluating sections of the scenario. Through these informal tests, bugs or discrepancies in the CyberCIEGE game engine or the SDT were discovered and reported. The majority of these discrepancies were fixed and released in an updated version of the CyberCIEGE game. Table 9 summarizes the key discrepancies in the game engine or SDT that were uncovered through these informal testes conducted during the development of the Operation Artemis scenario.

No.	Descriptions of Game Engine or SDT Bug	Resolution
1	The SDT's User DAC Group panel failed to display contents.	Fixed
2	There is a need to limit the number of words in the component description to prevent the CyberCIEGE game from crashing when the player purchases a component.	Fixed
3	Network connections not correctly displayed in the game's Network screen when the connected devices are not shown together on the screen.	Not Fixed
4	The SDT's Log file creator was corrupted. Asset attacks are reported in logfile.txt but can't be viewed in the Log Viewer.	Fixed
5	The SDT failed to execute Validate, Build and Run commands simultaneously due to a lack of memory.	Fixed
6	When an item is sold by the player, the item continues to graphically remain on the screen. Thus, screen remnants clean up is needed.	Fixed

No.	Descriptions of Game Engine or SDT Bug	Resolution
7	The users' thoughts generated by game engine were not meaningful.	Fixed
8	The asset goal description was truncated on the User screen	Fixed
9	The SDT does not recognize the reserved word '(PARAGRAPH)' in the objective description.	Not Fixed
10	Malicious software attacks on the assets failed to materialize even when the workstation connected to the assets is installed with low integrity software applications and there is a high attack motive of 501.	Fixed
11	The game engine renders similar character graphics for all the three male characters in the game.	Not Fixed
12	The game engine automatically halved the cost of asset being attacked when the asset was attacked a second time.	Not Fixed

Table 9.   Description of the discrepancies found and their resolutions, as of the publication of this thesis.

F.   SUMMARY

The testing methodologies and test cases discussed in this chapter verified that the Operation Artemis scenario is capable of achieving its intended security educational goals. The informal tests conducted during the scenario development process helped to uncover discrepancies in the SDT and the CyberCIEGE game engine, which led to fixes. These fixes significantly improved the functionality and usability of the SDT and the game engine.

The next and final chapter will provide recommendations and suggestions for future work for the CyberCIEGE project and will conclude the thesis.

VI. CONCLUSION AND RECOMMENDATIONS

This chapter provides recommendations, suggests future work for the CyberCIEGE project and concludes the thesis.

A. RECOMMENDATIONS

In the course of developing and testing the Operation Artemis scenario, some SDT and game engine discrepancies were encountered. These discrepancies and their resolutions were summarized in Table 9 of Chapter V. The following sections discuss the discrepancies that are yet to be resolved and should be addressed in the future updates of the game engine.

1. Network Connection

The network connections that exist among devices are shown graphically on the CyberCIEGE 'Network' screen. As shown in Figure 7, the connecting line between the devices is a graphical indication that these devices are interconnected. However, when the interconnected devices are not shown together on the same screen, as seen in Figure 8, the connecting line disappears. This graphical discrepancy of the game should be corrected to improve not only the playability of the game, but also to allow players to have a realistic depiction of the network connections.
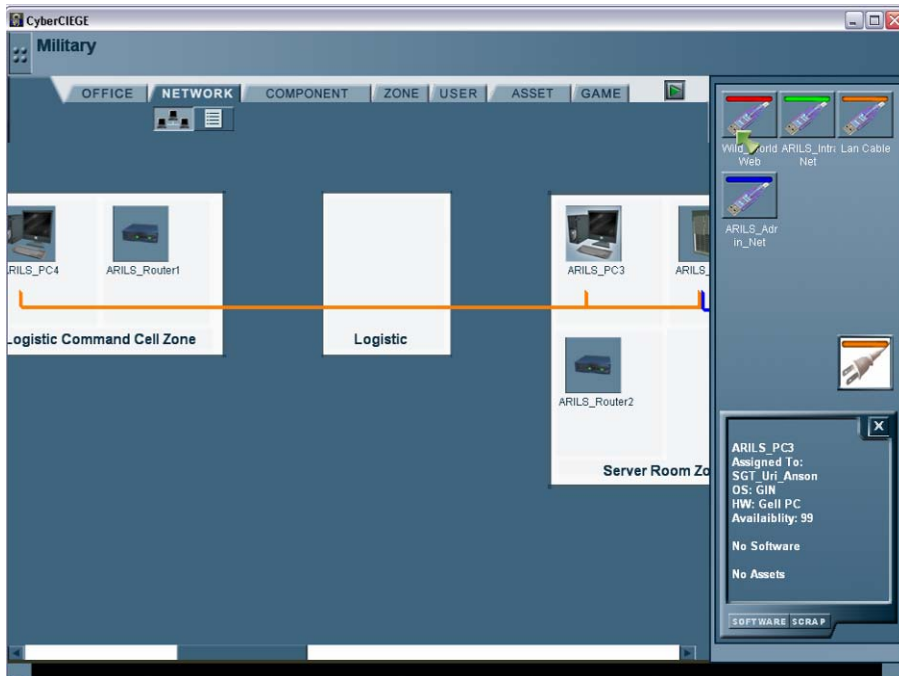
Figure 7.   Connecting line indicates interconnected devices.
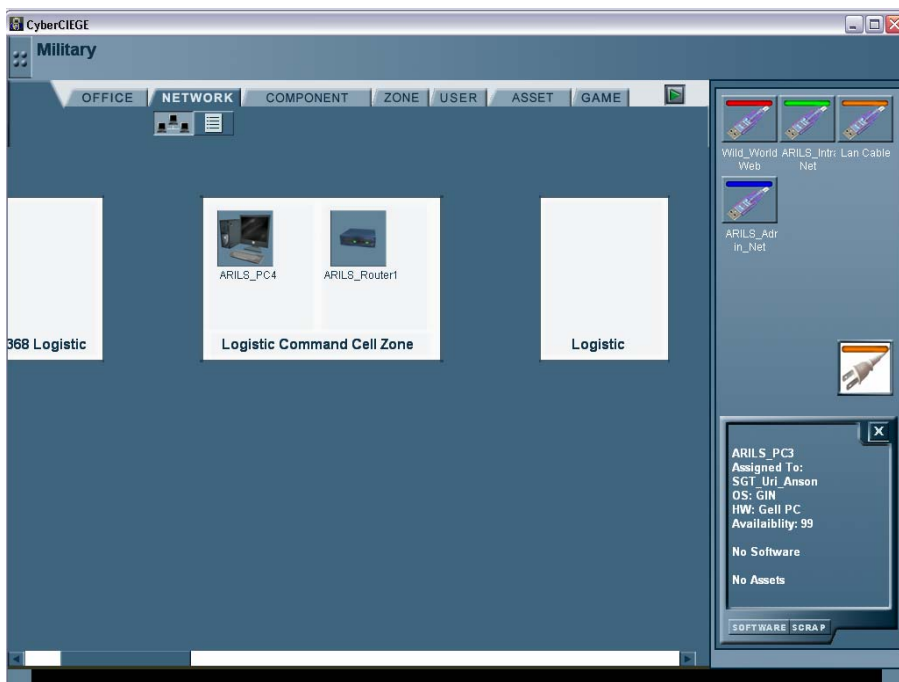

Figure 8.   Connecting line disappears.

2.   User Graphics

The CyberCIEGE graphic engine renders good three dimensional graphics of the characters in the game. However, these character graphics are limited in variety and are

not controllable by the scenario developers. Figure 9 shows MAJ Carson, WO Hector and SGT Anson, the three male characters of the Operation Artemis scenario, who, due to the graphics provided by the underlying game engine look graphically identical. Improvement to this graphical aspect of the game will improve the realism of the game. In addition, for military games, the graphics for the characters should include insignias and uniforms reflecting the appropriate rank of the users described.

Figure 9.   Operation Artemis triplets

3.   Cost of Attacks

The cost as a result of a malicious attack on an asset is set using the SDT. The value set will be the amount of money the player will lose when an attack occurs. If a similar attack happens again on the same asset, the game engine will automatically halve the cost of being attacked. This halving of the cost of being attacked is not controllable by the scenario developer and does not mimic the real-world situation well. It is suggested that the cost of subsequent attacks be controllable by the scenario developer. Improving this aspect of the game will improve its realism

4.   Software Component

Players can purchase or remove software components in CyberCIEGE by clicking on the 'Software' icon of the devices to invoke the 'Manage Software' screen. However, the description of the available software components can only be viewed by activating the CyberCIEGE encyclopedia. To improve the game play, it is suggested that the software description be made available through the 'mouse-over' or 'right-click' functions.

B.   FUTURE WORK

Due to the limited time available to complete this thesis, the 'Money' aspect of the CyberCIEGE game has not been fully exploited. Future work on the Operation Artemis scenario should involve the fine tuning on the use of 'Money' to create tension and sway the player's decision cycles. This will provide better realism and increase the challenge of the scenario.

A user trial should also be conducted with the completed Operation Artemis scenario on students from the NPS computer science department and DoD system administrators to check if the scenario fulfils the objective of conveying security lessons about the need of having software integrity and an air-gapped network architecture in a sensitive military environment.

C.   CONCLUSION

The Operation Artemis scenario developed for this thesis consists of five intriguing game phases that convey security lessons on the importance of software integrity in a sensitive military environment and the need of an air-gapped network architecture for mission-critical military backbone networks. With its successful development, the three thesis questions posed in the first chapter are answered.

The first thesis question asked if a scenario can be developed such that it is both playable and educational while illustrating the need for security and protection on mission critical data in a networked military environment? The answer to this question is yes. The development of Operation Artemis has demonstrated that CyberCIEGE, with its rich elements and tools, is capable of creating game scenarios that mimics real life IA issues and can be used for conveying security lessons to a wide audience of trainees.

The second thesis question asked whether a scenario can illustrate the tensions, trade-offs and decisions a network manager has to make when deciding between the use of an air-gapped network that is separated from the internet and the need for web connections? The fourth phase of Operation Artemis was developed to answer this question. In order to successfully complete this phase of the game, the player has to make

the decision to satisfy the users' desire for Internet connection by creating and maintaining a network that is strictly for Internet access only and totally separated from the air-gapped backbone network.

The third and final thesis question asked from the perspective of information assurance, to what extent is the use of commercial software on an air-gapped network comparable to connecting the network to the Internet, in terms of subjecting the network to possible malicious acts by adversaries? The third phase of Operation Artemis demonstrated that it is important to ensure that software applications running on a sensitive network are of trusted origin. Software products with low integrity can potentially corrupt the network and its high integrity systems. The installation of low integrity software on highly sensitive systems with an air-gapped network architecture exposes the systems to a high possibility of compromise which is similar to that of connecting the air-gapped network to the Internet.

The importance of Information Assurance (IA) in military operations cannot be overstated. In its quest to safeguard its information systems, the military faces the same risks and challenges as any other government or private sector organization that has heavy reliance on today's wired world. The provision of security education to all personnel in the organization is critical to achieving IA. This thesis demonstrated that CyberCIEGE, with its rich elements and tools, can be used to create game scenarios, mimicking real life IA issues, for conveying security lessons to a wide audience of trainees. It provides an excellent alternative to traditional methods of security education which often fail to drive home the intended lessons.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[Cerf 2004]   Vinton G. Cerf, *A Brief History of the Internet and Related Networks.*
                     Accessed on August 2005. URL:
                     http://www.isoc.org/internet/history/cerf.shtml

[Leiner 2003]   Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn,
                     Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts,
                     Stephen Wolff, *A Brief History of the Internet*.
                     Accessed on August 2005. URL:
                     http://www.isoc.org/internet/history/brief.shtml

[GAO 1996]   *Information Security: Computer Attacks at Department of Defense
                     Pose Increasing Risks*, May 1996
                     Accessed on September 2005. URL:
                     http://www.fas.org/irp/gao/aim96084.htm

[GAO 2000]   *FAA Computer Security, Actions Needed to Address Critical
                     Weaknesses That Jeopardize Aviation Operations*, September 2000
                     Retrieved on August 2005. URL:
                     http://www.gao.gov/new.items/ai00330t.pdf

[Kessler 1997]   Gary C. Kessler and Carol A. Monaghan, *Considerations for LAN
                     and Internet Security*. February 1997
                     http://www.garykessler.net/library/secure.html

[Ryan 1997]   Daniel J. Ryan*, INFOSEC and INFOWAR: Considerations for
                     Military Intelligence*.
                     Accessed on September 2005. URL:
                     http://www.danjryan.com/MIntl.html

[NSTSC 2003]   *The National Strategy to Secure Cyberspace,* February 2003
                     Retrieved on August 2005. URL:
                     http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[Irvine1 2003]   Cynthia E. Irvine and Michael Thompson, *Teaching Objectives of
                     a Simulation Game for Computer Security*, June 2003
                     Retrieved on August 2005. URL:
                     http://cisr.nps.navy.mil/cyberciege/downloads/CyberCiege_ISIT.pdf

[Irvine2 2005]   Irvine, C.E., Thompson, M.F., Allen, K., CyberCIEGE: Gaming for Information Assurance, Naval Postgraduate Sch., Monterey, CA, USA; Security & Privacy Magazine, IEEE, May-June 2005, Volume: 3, Issue: 3, page(s): 61- 64, ISSN: 1540-7993

[Kirriemuir 2002]   Kirriemuir, J. (2002). *Video Gaming, Education and Digital Learning Technologies. D-Lib Magazine.*
Accessed on August 2005. URL:
http://www.dlib.org/dlib/february02/kirriemuir/02kirriemuir.html

[Angiolillo 2005]   Paul Angiolillo, *TechnologyReview.com: Gaming Makes the Grade*. September 2005
Accessed on September 2005. URL
http://www.technologyreview.com/articles/05/09/wo/wo_092705a ngiolillo.1.asp

[Johns 2004]   Johns, K., 2004, Toward Managing & Automating CyberCIEGE Scenario Definition File Creation, NPS, Monterey, 2004

[FCW1 2005]   *Federal Computer Week, FCW.com, The New Trojan war Defense Department Finds its Networks under Attack from China,* Frank Tiboni, Published on Aug. 22, 2005
Accessed on August 2005. URL
http://www.fcw.com/article90262-08-22-05-Print

[NSTISSI 4009]   *NSTISSI No. 4009, National Information Systems Security (INFOSEC) Glossary,* September 2000, National Security Telecommunications and Information Systems Security Committee of the United States
Retrieved on September 2005. URL:
http://security.isu.edu/pdf/4009.pdf

[Webopedia 2005]   Webopedia, online dictionary and search engine for computer and Internet technology definitions, 2005
Accessed on September 2005. URL
http://www.webopedia.com/

[Jackson 2002]   Frederick E. Jackson, *Tannenberg: The First Use of Signals Intelligence in Modern Warfare*.
Retrieved on August 2005. URL:
http://www.iwar.org.uk/sigint/resources/sigint/Jackson_F_E_02.pd f

[FCW2 2005]   Mary Ann Davidson, *Federal Computer Week, FCW.com Lessons
                   of Warfare for IT Security*.
                   Published on October 17, 2005
                   Accessed on October 2005. URL:
                   http://www.fcw.com/article91127-10-17-05-Print

[IT PRO 2005]   Michael, J.B.; Roberts, S.E.; Voas, J.M.; Wingfield, T.C.; *IT
                   Professional, The role of policy in balancing outsourcing and
                   homeland security.* Volume 7, Issue 4, July-Aug. 2005 Page(s):19 -
                   23

[GAO 2004]   *DEFENSE ACQUISITIONS Knowledge of Software Suppliers
                   Needed to Manage Risks*, May 2004
                   Retrieved on September 2005. URL:
                   http://www.gao.gov/new.items/d04678.pdf

[Safire 2004]   *The Farewell Dossier*, W. Safire, The New York Times, 2 Feb.
                   2004. p.A21.

[DCMil 2005]   Joseph Gunder, *The Waterline, Navy Improves Network Security
                   by Blocking Access to Webmail*. October 27, 2005
                   Accessed on October 2005. URL:
                   http://www.dcmilitary.com/navy/seaservices/10_43/national_news/
                   37851-1.html

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
    Ft. Belvoir, Virginia

2. Dudley Knox Library
    Naval Postgraduate School
    Monterey, California

3. Ken Allen
    Rivermind, Inc
    Mountain View, California

4. Hugo A. Badillo
    NSA
    Fort Meade, Maryland

5. George Bieber
    OSD
    Washington, DC

6. RADM Joseph Burns
    Fort George Meade, Maryland

7. John Campbell
    National Security Agency
    Fort Meade, Maryland

8. Deborah Cooper
    DC Associates, LLC
    Roslyn, Virginia

9. CDR Daniel L. Currie
    PMW 161
    San Diego, California

10. Louise Davidson
    National Geospatial Agency
    Bethesda, Maryland

11. Vincent J. DiMaria
    National Security Agency
    Fort Meade, Maryland

12. Scott Gallardo
Rivermind, Inc
Mountain View, California

13. Jennifer Guild
SPAWAR
Charleston, South Carolina

14. Richard Hale
DISA
Falls Church, Virginia

15. LCDR Scott D. Heller
SPAWAR
San Diego, California

16. Wiley Jones
OSD
Washington, DC

17. Russell Jones
N641
Arlington, Virginia

18. Steve LaFountain
NSA
Fort Meade, Maryland

19. Dr. Greg Larson
IDA
Alexandria, Virginia

20. Gilman Louie
In-Q-Tel
Menlo Park, California

21. Ernest Lucier
Federal Aviation Administration
Washington, DC

22. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, Virginia

23. Dr. Vic Maconachy
    NSA
    Fort Meade, Maryland

24. Doug Maughan
    Department of Homeland Security
    Washington, DC

25. Dr. John Monastra
    Aerospace Corporation
    Chantilly, Virginia

26. John Mildner
    SPAWAR
    Charleston, South Carolina

27. Jim Roberts
    Central Intelligence Agency
    Reston, Virginia

28. Keith Schwalm
    Good Harbor Consulting, LLC
    Washington, DC

29. Dr. Ralph Wachter
    ONR
    Arlington, Virginia

30. David Wennergren
    DoN CIO
    Arlington, Virginia

31. David Wirth
    N641
    Arlington, Virginia

32. Daniel Wolf
    NSA
    Fort Meade, Maryland

33. Jim Yerovi
    NRO
    Chantilly, Virginia

34. Dr. Cynthia E. Irvine
    Naval Postgraduate School
    Monterey, California

35. Paul C. Clark
    Naval Postgraduate School
    Monterey, California

36. Michael Thompson
    Naval Postgraduate School
    Monterey, California

37. Professor YEO Tat Soon
    Director of Temasek Defence Systems Institute
    National University of Singapore, Singapore

38. Ms Tan Lai Poh
    Senior Admin. Officer of TDSI
    National University of Singapore, Singapore

39. Chay Chua
    Student, Naval Postgraduate School
    Monterey, California