NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBERCIEGE SCENARIO ILLUSTRATING SECRECY ISSUES IN AN INTERNAL CORPORATE NETWORK CONNECTED TO THE INTERNET

by

Justin D. Lamorie

September 2004

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** September 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) A CyberCIEGE Scenario Illustrating Secrecy Issues in an Internal Corporate Network Connected to the Internet.			**5. FUNDING NUMBERS**
6. AUTHOR(S) Justin D. Lamorie			
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 CyberCIEGE project seeks 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. The game provides a robust, flexible and extensible gaming environment where each game instance is based on a fully customizable scenario.

These customized scenarios produce game simulations that are tailored to meet a player's specific IA training needs, thus providing personalized, focused IA training at a minimum cost in both dollars and time. Additionally, the interactive game simulations, provided by the CyberCIEGE game, create an entertaining and realistic training environment for the player. Finally, the ability to load the game onto, and execute it from a PC allows IA training to be conducted practically anywhere, i.e. at home, or while traveling.

To demonstrate this capability, this thesis developed a customized scenario designed to educate players in secrecy issues concerning the connection of an internal corporate network with the Internet. Additionally, this thesis produced Scenario Definition Files (SDFs) designed to test the game engine to determine if it would produce results that met the SDF developer's expectations and that the simulated game environment was realistic.

14. SUBJECT TERMS Information Assurance, CyberCIEGE, Scenario Definition File, Network Security Training			**15. NUMBER OF PAGES** 106
			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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

A CYBERCIEGE SCENARIO ILLUSTRATING SECRECY ISSUES IN AN INTERNAL CORPORATE NETWORK CONNECTED TO THE INTERNET

Justin D. Lamorie
Captain, United States Marine Corps
B.S., Arizona State University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2004

Author: Justin D. Lamorie

Approved by: Cynthia E. Irvine
Thesis Co-Advisor

Paul C. Clark
Co-Advisor

Michael F. Thompson
Second Reader

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The CyberCIEGE project seeks 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. The game provides a robust, flexible and extensible gaming environment where each game instance is based on a fully customizable scenario.

These customized scenarios produce game simulations that are tailored to meet a player's specific IA training needs, thus providing personalized, focused IA training at a minimum cost in both dollars and time. Additionally, the interactive game simulations, provided by the CyberCIEGE game, create an entertaining and realistic training environment for the player. Finally, the ability to load the game onto, and execute it from a PC allows IA training to be conducted practically anywhere, i.e. at home, or while traveling.

To demonstrate this capability, this thesis developed a customized scenario designed to educate players in secrecy issues concerning the connection of an internal corporate network with the Internet. Additionally, this thesis produced Scenario Definition Files (SDFs) designed to test the game engine to determine if it would produce results that met the SDF developer's expectations and that the simulated game environment was realistic.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

DAC	Discretionary Access Control
DoD	Department of Defense
DoS	Denial of Service
IA	Information Assurance
IT	Information Technology
MAC	Mandatory Access Control
SDF	Scenario Definition File

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The successful completion of this thesis would not have been possible were it not for the support of many individuals.

I would first like to thank my wife, Alicison, and our children, Cole and Cael, for their love and support. Thank you for tolerating my many absences from our family and supporting me in accomplishing my goals.

I would like to thank Dr. Cynthia Irvine, Paul Clark and Mike Thompson, my advisory team. Your insight, guidance, comments and support have been invaluable in completing this thesis and have made it what it is today.

To Mark Meyer, Rob LaMore, Ken Johns, JD Fulp, and Daniel Warren. You have all been good friends and mentors, thank you for insight, wisdom and camaraderie.

I would like to send a special thank you to Klaus Fielk. Without your help, camaraderie, organizational skills, and above all else your friendship this thesis and my time here at NPS would not have been as worthwhile an experience.

Finally, I would also like to thank Gary Kreeger, and Jean Brennen for the excellent support you provided me as a student during my academic career at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

The purpose of this thesis is to develop a playable CyberCIEGE scenario that provides security training and education in a new and more entertaining fashion. Specifically this thesis will produce a scenario that illustrates some of the issues associated with connecting an internal network to the Internet. The results of this thesis will contribute to the mission of the current CyberCIEGE project being conducted at the Naval Postgraduate School, Monterey California. The CyberCIEGE project mission is to "create an Information Assurance (IA) teaching/learning laboratory". [Irvine 2003] This thesis will provide the CyberCIEGE project with a playable game scenario customized to focus its training on a specific aspect of IA and numerous test scenarios that will test the CyberCIEGE game engine's ability to produce results that meet the scenario developer's expectations. These results will provide valuable research that, in conjunction with the rest of the CyberCIEGE project, will facilitate the final goal of the overall project.

To conduct this thesis two questions must be asked and answered. First, can a CyberCIEGE scenario be developed such that it is simultaneously a playable game and an educational tool that illustrates confidentiality issues in an internal corporate network connected to the Internet? Second, is it possible to validate that the CyberCIEGE game engine produces expected results from a predefined[1] scenario definition file. By answering these questions, the usability and flexibility provided by a scenario definition file as well as the performance of the game engine will be validated and thus will help advance the goals of the CyberCIEGE project.

B. THESIS SCOPE

To answer the first question posed, this thesis will provide a playable CyberCIEGE game scenario, utilizing *Scenario Definition Files (SDF),* that illustrate the issues involved with ensuring information confidentiality in a networked computer system environment. Additionally, to answer the second question, this thesis will provide

[1] Predefined in relation to a Scenario Definition File refers to a file in which all game play decisions have been made prior to executing the game simulation.

a test strategy for validating that the CyberCIEGE game engine produces results, from a predefined SDF, which both meets preconceived expectations and produces a game simulation that unfolds in a realistic and acceptable manner.

C. CHAPTER OVERVIEW

This thesis will be developed in six chapters. The thesis chapters will be laid out in the following order:

- Chapter I - Introduction – This chapter will introduce the project and discuss the motivation behind this thesis.
- Chapter II – Background – This chapter will provide the background information necessary to understand this thesis.
- Chapter III – Scenario Goals – This chapter describes the intended audience for the CyberCIEGE game as well as the specific educational goals of the SDF included.
- Chapter IV – Scenario Description – This chapter will describe, in detail, the playable game scenario that was developed for this thesis. It includes a narrative description of the "virtual world" that is being modeled as well as a description of the users, policies, assets, components, and potential attacks.
- Chapter V - Testing – The testing methodology, test cases, and test results will be discussed.
- Chapter VI - Future Work & Conclusion – This chapter will suggest potential areas for further research, as well as some final thoughts on the project and its success.

D. APPENDIX OVERVIEW

The following appendices will be attached to this thesis:

- Appendix A – Test Cases – These test cases focused on determining if scenarios could be written in which a classified asset could be secured using physical or procedural security measures. Numerous test cases were conducted, each of which was designed to determine if the game engine performed in an acceptable manner and that SDF could be configured to produce outcomes that met expected results.
- Appendix B – *VentureGames* Scenario – The *VentureGames* Scenario is the playable game scenario developed for this thesis. It is composed of five individual game modules, each of which builds on lessons learned from the previous modules.

- Appendix C – *VentureGames* Scenario Solutions – These SDFs provide a winnable solution to each of the *VentureGames'* modules.

E. SUMMARY

This chapter has identified the focus of this thesis and informed the reader of the two basic questions this thesis will attempt to answer. Additionally, this chapter defines the scope of the thesis and identifies, to the reader, what end products are expected upon the successful completion of this thesis. Finally, this chapter provides the reader with an outline and brief description, of the contents, of each chapter and appendix contained in this thesis. The following chapters will expound on the topics covered in this chapter and attempt to answer the questions posed.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. THE NEED FOR INFORMATION ASSURANCE TRAINING

We live in an amazing time in the annals of human history: the Information Age. Recent technology has provided immeasurable advantages over past generations with regard to the dissemination, processing, and storage of information, such as global communications networks, computers, and the Internet. This technology has also introduced numerous new challenges to the protection of information from unauthorized access and modification. These new challenges must be addressed in order to support Information Assurance. Formally Information Assurance is defined as:

> Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. [CNSS 2003]

A fundamental step required to protect information, whether it is a nation's top-secret nuclear technology or a small business' accounting data, is to provide training in Information Assurance to the users of this information. Prior to the invention of computers, physical security means such as safes, locked filing cabinets, and secured rooms were used to protect information. The development of the first generation of digital computers, in the United States following World War II [Britannica], introduced new information protection challenges in the areas of unauthorized access and modification of protected information. The explosive growth in users of the Internet, estimated to be 1.10 billion by 2005 [ClickZ 2004], and the increased reliance, by both corporate and military sectors, on networked computing systems to process, store, and disseminate their information have introduced even greater challenges to information protection.

In today's high technology fast-paced society the ability to instantly and reliably access information is so ubiquitous that it has become a necessity, for both personal and professional uses, rather than a luxury. Simply isolating it, either in a safe or secure room or on a stand-alone computer system, can no longer solely protect information. Information's value comes from its authorized users' ability to access it and then process it in conjunction with any other information available to those users. The need to process

different information, with different security attributes, simultaneously leads to the intermingling of information needs. Cleared users often need access to low sensitivity information at the same time that they need access to highly sensitive information. Thus users may need a single system to store and protect both unclassified and classified information. This requirement introduces several new security concerns such as security labels, and access controls. Additionally, the requirement to access information via a network introduces even more challenges to securing information. To protect information from the new vulnerabilities introduced by technological advances, numerous protection mechanisms are often employed. These protection mechanisms can be in the form of physical security measures, procedural security measures, and/or technical security measures. This is also where the need for user training comes in. Whether by intentional or accidental means, users often pose the greatest threat to information assurance today. [Southgate 2002]

Training and education, however, are troublesome and often difficult requirements to meet. Security is a complex topic that encompasses interrelated concepts and mechanisms that must be combined properly to ensure protection for information. The models and mathematics behind these topics and concepts are often far beyond the grasp of the average user. Traditional pedogical techniques often fall short of fulfilling the security teaching objectives required for today's information user. PowerPoint briefs and mass email reminders are treated as more of a nuisance than as useful security training material. Long technical seminars and formal classes that describe every nuance of security policies and technologies are not appropriate for the average user and are often far beyond their comprehension. So what is the answer?

What if there was a training tool that would simultaneously educate while it entertained the user? What if this tool could simulate the real world and the issues involved in Information Assurance and could be configured so that it could be used in a formal classroom setting as well as on a home PC? What if personalized scenarios could be developed that focus on a particular security aspect or need? What if this tool could be scaled so that it could train every level of user, from entry-level personnel to security experts? What if this tool came in the form of "an interactive, entertaining, commercial-grade PC-based computer game where players construct and defend a networked

computing system?" [Cyber 2003] This is the potential that the CyberCIEGE project brings to the security training table.

B. THE CYBERCIEGE VIRTUAL LABORATORY

The following section provides a synopsis of [Cyber 2003]. The Naval Postgraduate School's (NPS) Center for Information Systems Security Studies and Research (CISR) has taken on these "what ifs" and begun the development of just such a tool. It will address many of the issues previously mentioned concerning Information Assurance and network security. In order to ensure the highest quality product possible, CISR has joined forces with Rivermind, a professional game development company. Together CISR and Rivermind have developed CyberCIEGE, an Information Assurance (IA) teaching/learning laboratory that integrates rigorous scientific foundations with the application of abstract principles to the real world. This hands-on virtual laboratory will provide a dynamic and surprising context from which abstract principles can be discovered and then applied. By packaging this information assurance laboratory as an interactive, entertaining, commercial-grade PC-based computer game, CyberCIEGE will be able to package much-needed education/training into an entertaining and user-friendly environment. The players will be able to construct and defend a networked computing system by selecting information technology resources to meet the explicit needs of virtual "users", and defend the resulting system from numerous threats.

1. Game Play

Conceptually CyberCIEGE is a resource management video game similar to other simulation games currently on the market except that, rather than allowing players to choose rides, refreshments and facilities, CyberCIEGE will enable players to create and control computer networks, implement security measures, hire and fire IT staff and defend the network. Players will learn through choices they make. Poor security choices will result in unintended results. To be successful in the game, the player will have to identify vulnerabilities, make sound Information Assurance choices, and maintain the network's security. The entertainment aspect of the game is derived from the interaction between the game engine and the player. Once the player believes that all of the

appropriate security measures have been taken and that the information is safe, the game engine starts to probe the security defenses chosen by the player until vulnerabilities lead to unintended consequences. The player must then identify and resolve these newly discovered vulnerabilities, in order to protect the information, never knowing if any new security decision will open even more unforeseen vulnerabilities.

2. Virtual Laboratory

In addition to being a commercial-grade PC-based video game, CyberCIEGE can act as an Information Assurance virtual laboratory. Establishing a traditional laboratory network is not always possible in a training environment. Financial, spatial, and time constraints often restrict the instructor's ability to provide students with "hands on" training which is often critical to true understanding and appreciation for the nuances associated with securing complicated network architectures. As a virtual laboratory, instructors will be able to augment classroom instruction with training provided by the simulations of the CyberCIEGE game. The training provided by CyberCIEGE results from the game engine's ability to identify security lapses in policy, procedure, training, or execution, and then simulate probable attacks that would occur due to these security lapses. Players will "pay a price" for these security lapses until they identify the problem and take appropriate actions to resolve the situation. The non-deterministic nature of the game ensures that repeated executions of the same scenario will result in a variety of outcomes.

Training via a virtual laboratory has several obvious advantages over training on a physical laboratory network. First, the game can be tuned to any level of training needed. CyberCIEGE can provide simulations that cover basic concepts, for entry-level students, to advanced topics, for advanced technical security experts. Second, the game is interactive in that it will provide feedback to the student and the instructor in the form of pop-up and banner messages during game play and "log" and "results" files after the game is completed. The "log" and "results" are critical to the training process for they provide both the instructor and student with the ability to evaluate the student's performance and to identify those vulnerabilities unmitigated by the student that the game engine recognized and took advantage of. This immediate access to feedback ensures

that the errors the student made in establishing security policy or procedure within the CyberCIEGE simulation can be both explained to the student and corrected in a timely manner.

C. THE NEED FOR CUSTOMIZABLE SCENARIOS

Traditionally PC-based video games come packaged with a limited number of scenarios that a player can choose from. These scenarios are often played in a fixed sequence. In order to prevent players from becoming disinterested and to capitalize on brand loyalty, game developers often offer "expansion packs" to their games. These expansion packs are in essence additional scenarios that the player can add to the original configuration in order to extend the playability of the game. These "expansion packs" are also instrumental in introducing new characters, concepts, and capabilities. However, the player has no say in what these improvements to the game will be, when they will be offered, or even which game improvements they want to utilize. What if the scenario details could be tailored to meet the player's specific game preferences or training requirements?

The training advantage provided by the CyberCIEGE game architecture is derived from its ability to develop and accept customizable scenarios. As defined by the CyberCIEGE encyclopedia a scenario is "an instance of the CyberCIEGE game in which the player is given an initial budget and succeeds by reaching a defined objective." [Rivermind2 2002] The game is able to run these customized scenarios through the use of a SDF. The SDFs provide both players and instructors with the ability to choose the scenario's startup information. This startup information includes such things as which users to include, what assets are needed, the goals, the win/loss conditions, and numerous other choices. These player-determined choices are what provide the variety, complexity, and uniqueness to each of the customized scenarios. SDFs provide the means through which the player can make scenario game play choices and then, in a game-readable format, enter those choices into the CyberCIEGE game engine. This format has been developed into a template known as the Scenario File Template (SFT). As described by [Johns 2004] "the SFT is the master document that describes the scenario language and how it is to be used to create scenarios. It specifies the layout of an SDF, in what order

fields are expected to appear, what is optional and what is not." A more detailed explanation of the SFT is given by [Johns 2004].

The scalability provided by this ability to develop customizable game scenarios is what makes CyberCIEGE a breakthrough in Information Assurance training. A single CyberCIEGE game engine can be used to train both entry-level Information Assurance students and advanced technical security experts. The game engine can easily be configured to simulate fundamental security issues in a step-by-step manner, and then simulate highly complex, and often obscure, security concepts. Focused training on specific aspects of Information Assurance and broad overview training can both easily be accommodated simply by loading a customized scenario into the game engine.

D. KEY CONCEPTS

For the reader to fully understand what is taught in the scenario provided with this thesis, some key security concepts must be covered. This review will provide a basis for understanding why certain security decisions were made and the significance of the outcome of the game's execution. The following definitions for Information Assurance and Network Security provide a basis from which the rest of the concepts can expand.

The National Information Assurance Glossary defines Information Assurance as:

> Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [CNSS 2003]

Additionally computer security is defined as:

> Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored and communicated. [CNSS 2003]

The concepts in these two definitions overlap. Key aspects that must be understood are those of confidentiality, integrity, and availability.

1. Security Policy

A security policy is the foundation for protecting information. As defined by the CyberCIEGE encyclopedia:

> A security policy is a set of laws, rules, and practices that regulate how an enterprise manages, protects, and distributes sensitive information. [Rivermind2 2004]

Security policies are complex documents that outline the steps and procedures required to protect information. This thesis will focus on the following areas of a security policy:

- Physical Security – Physical security encompasses a wide variety of security measures. These measures range from installing locks on doors to hiring guards and installing surveillance cameras. Physical security also includes measures such as developing a contingency plan in case of a natural disaster or providing back-up power in case of a power blackout. A basic definition of physical security as it relates to computer security is "controlling the comings and goings of people and materials; protection against the elements and natural disasters." [Albion 2004]
- Mandatory Access Control – Typically a management directive that identifies the sensitivities of information and the constraints placed on people who might have access to the information. Access is not granted based on the discretion of individual users. These "MAC" policies are both global and persistent. Example uses of MAC policies are protection of highly proprietary secrets from potential competitors and ensuring that only authorized accountants can alter specific critical financial data." [Rivermind2 2004]
- Discretionary Access Control – Individual users or groups of users can own or otherwise control the access to information and potentially the dissemination of rights to grant access to other users. Access decisions are based on the discretion of users (often within the context of management mandates intended to constrain a user's decision to grant access based on a "need to know"). [Rivermind2 2004]

There are numerous other security issues and countless details involved in developing and implementing a security policy. The CyberCIEGE encyclopedia, [Rivermind2 2004], provides more detail on security policies and how they relate to the CyberCIEGE game.

2. Confidentiality

Confidentiality is the key aspect of information assurance for this thesis therefore a formal definition is provided so that the reader has a basis of understanding. Confidentiality is:

> Assurance that information is not disclosed to unauthorized entities or processes. [CNSS 2003]

The need to protect information from unauthorized access ranges from the requirements of nation states all the way down to those of a single individual on a personal computer. This information could be as mundane as secret chicken recipe or as sensitive as the technical specifications for construction of a centrifuge to enrich uranium. Confidentiality relates to the requirement that these "secrets" are protected. The focus of this thesis is to develop a CyberCIEGE scenario that simulates the confidentiality issues involved in protecting classified corporate information within an internal network connected to the Internet. To develop this scenario, several concepts important to understanding how the confidentiality of information is protected must be discussed.

3. Integrity

Integrity is a key aspect of information assurance and computer security. Formally, integrity is defined as:

> The quality of an 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. [CNSS 2003]

The importance of the integrity of information cannot be overstated, for example a small error in a map grid coordinate entered into a cruise missile's guidance system could have catastrophic effects. The integrity of information can be paramount to the success of the user of that information. However, for this thesis, integrity is not the focus of the scenario. A CyberCIEGE scenario that focuses on integrity is being developed elsewhere.

4. Availability

The availability of information is a simple concept to grasp, but is difficult to achieve. Availability is formally defined as:

> The prevention of unauthorized withholding of information or resources. [CNSS 2003]

What availability means, as it relates to information, is that access to the information is attainable at a desired time. The most common term associated with availability is Denial of Service (DoS). DoS is the "type of incident resulting from any action or series of actions that prevents any part of an IS from functioning." DoS attacks are often thought of as being the type conducted by hackers against websites that they may disagree with, however, DoS attacks come in many more variations. Loss of electrical power, overloaded bandwidth, and password lockouts are all common examples of DoS attacks. Availability issues are not the focus of the scenario developed for this thesis. The issues involved with availability will be modeled and developed elsewhere within the context of the CyberCIEGE project.

5. Networks

A network is "a group of two or more computer systems linked together." [Webopedia 2004] Networks have many topologies (hub, star, ring, etc.) and sizes (LAN, MAN, WAN, etc.) and are used for many purposes (military, corporate, commercial, etc.) To keep this thesis to an appropriate scale only two types of networks will be considered. The first is an internal network, which is often called an *intranet*. Intranets are closed networks that belong to an organization and only authorized users can gain access to it. The second network considered is the Internet. The Internet is the largest inter-networking of computers in the world. It spans virtually every country and continent and is accessible to billions of people each day. In the past ten years the Internet has become so integrated into peoples lives that it has become indispensable in modern society. [Hoffman 2004] The following formal definition of each of these types of networks is provided for the reader to establish a basic understanding of the key aspects of each.

An intranet is defined as:

> 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 2004]

The Internet is defined as:

> 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 2004]

Networks have been an instrumental part of the technological revolution that has brought about an age of information. Today information has become the most valuable and sought after commodity in the world. Those who have it, or can get it, often have an insurmountable advantage over those who do not. This is true in both the commercial and military sectors. Thus, the need to protect information from unauthorized access has become of paramount importance to those who covet it.

6. Components

To facilitate the confidentiality of classified information numerous components have been created that play a role in ensuring the confidentiality of protected information. These components, workstations, servers, routers, and firewalls, are often the key nodes in both corporate and military information infrastructures and thus are often points of vulnerability. A brief definition of each of the key components required for this thesis is provided to provide a basis of understanding for the reader.

Workstation - A workstation is equivalent to a modern day personal computer. They are the backbone of today’s corporate and military work environment.

Workstations can store assets locally, i.e. on the workstation itself, or they can be used to access assets that are stored on other components connected to the workstation via networks. [Rivermind2 2004]

Server - Servers are the worker bees of a network. They contain and often provide much of the information that people are interested in. A server is primarily used to store assets and host application programs (e.g., resource management programs). At a minimum, servers can be used to store and share assets. Servers can include specific applications that provide the functions of other components, e.g., a server with an e-mail application looks like an e-mail server. [Rivermind2 2004]

Router – Routers link local networks with remote networks. Routers provide a means of interconnecting multiple distinct networks that are potentially of different physical types (e.g., connect LANs with wide area networks such as the Internet). Routers include one or more "internal" networks and one "external" network connection. External connections can only be interconnected to other router external connections. Routers include filters such that traffic flow between the networks is constrained based on the type of the destination application. For example, a router can permit or deny Web access requests (HTTP) flowing to the external network from the internal network or flowing from the external network form the internal network. [Rivermind2 2004]

Firewall – Firewalls are network security devices designed to logically separate physically connected networks, such as separating an intranet from the Internet. In corporate networks firewalls provide a means of interconnecting the "internal" corporate network to an "external" network such as the Internet. To facilitate this separation firewalls include filters such that traffic flow between the networks is constrained based on the kind of application to which the traffic is destined. For example, a firewall can permit or deny Web access requests (HTTP) flowing to external network from the internal network and/or flowing from the external network from the internal network. Firewalls also potentially include other traffic filtering functions such as virus detection. [Rivermind2 2004]

E. SUMMARY

This chapter has provided the reader with background information detailing the need for Information Assurance (IA) training in both corporate and military computing environments. Second, this chapter has provided the reader with a description and explanation of both the purpose and goal of the CyberCIEGE project. Third, this chapter has informed the reader of the importance of the ability of the CyberCIEGE game to accept and execute customizable game scenarios. These customized game scenarios facilitate individualized and focused IA training, at minimum cost in both money and time. Finally, this chapter has provided the reader with both explanations and definitions of some key concepts, such as confidentiality, and aspects of network topologies, of Information Assurance and network security necessary for understanding subsequent chapters in this thesis. Additional details concerning these notions, as well as issues concerning game play, are more thoroughly addressed in the CyberCIEGE encyclopedia.

III. SCENARIO GOALS

A. INTENDED USERS

In general, the intended users for the CyberCIEGE game are DoD employees, both civilian and military personnel. The DoD has an immense requirement to provide information confidentiality and network security due to the nature of information it deals with on a daily basis. In order to protect this information the DoD spends millions of dollars annually on systems, software, procedures, and equipment that are designed to meet these requirements. But even the most secure system has some vulnerability and more often than not it is the personnel themselves whose behavior can introduce vulnerabilities. The concepts and procedures involved with ensuring the confidentiality of information are very complex and often cumbersome. The requirement to train personnel in these concepts and procedures is a daunting task. The DoD directly employs over 2 million personnel [DIOR 2004] and works with millions more in the form of contractors, researchers, advisors, and consultants. All of these people require Information Assurance (IA) training. However, they often require different levels and aspects of this training because people often possess different degrees of inherent knowledge and previous training experience. These differences must be taken into account when developing an IA training program. If the training is too difficult the students will not grasp the concepts being taught making the training useless and a waste of valuable time. Additionally, if the training is below the students level of inherent knowledge the student will become bored and uninterested and once again the training evolution becomes a waste of time.

The ability to customize training to an individual person's needs has, to this point, been both economically and logistically impossible, especially for an organization the size of the DoD. The CyberCIEGE game addresses this need and provides a means for conducting individualized training so that it is cost efficient, timely, and entertaining. The CyberCIEGE game allows for training to be conducted by anyone, anytime, and anywhere that they can access a personal computer. With CyberCIEGE training would no longer have to interrupt personnel schedules and work days; it can simply be completed while personnel are conducting their everyday routines. Additionally training

can be completed while students are at home, on temporary additional duty, or while traveling.

The specific intended users of the CyberCIEGE game and associated scenario definition files are the instructors that are required to provide training and the players who are required to receive the training.

1. Instructor

CyberCIEGE Virtual Laboratory instructors come in many forms. They can be traditional instructors who conduct training in formal school environments or they can be system administrators who manage small office networks. In either case they are the ones charged with providing Information Assurance training to their users. CyberCIEGE provides them with a scalable, customizable, and entertaining way of conducting this training, whether required or voluntary.

The key aspect of the CyberCIEGE game for instructors is the ability to produce customized Scenario Definition Files (SDF). These customized SDFs provide instructors with the ability to develop training scenarios that focus on topics and concepts that an individual student may require and to provide this training in an entertaining and educational environment. Additionally, the random nature of the game allows for numerous outcomes from the same scenario. For example a confidential asset may be protected from an external attack in one execution of the scenario while the same confidential asset may be compromised by an internal attack in a subsequent execution of the game. This aspect of the game provides the instructor with a tool that demonstrates the random nature of the types of attacks the player must contend with.

2. Player

The targeted player of the CyberCIEGE game is anyone requiring access to a DoD computer or network. Players can be organized into several groups. These groups include:

- New personnel with little or no initial training in computer security
- Transferred personnel who have some security awareness training

- Current personnel requiring annual refresher training
- Information Technology personnel requiring continuing education
- Personnel requiring training in order to regain suspended network privileges
- Personnel attending formal schools

The benefit CyberCIEGE brings to the training table for the players is that the games can be tailored to the player's skill levels and training requirements. They can play the game wherever and whenever they have access to a personal computer, thus avoiding daylong training seminars.

B. EDUCATIONAL GOALS

The goal of this thesis is to provide a SDF that is simultaneously a playable game and an educational tool that illustrates some specific concepts associated with information confidentiality. For this thesis, the scenario being developed is focused on providing training for inexperienced or entry-level personnel; therefore, a sequential, modular approach to game development was taken. Additionally, due to the vast array of topics associated with the confidentiality of information, three specific issues will be focused on in this thesis. The confidentiality issues covered in this thesis encompass those issues involved with providing physical security for information, and establishing internal network connections (i.e. Intranet), and external network (i.e. Internet) connections to access information. The scenario developed for this thesis will provide training in these topics by utilizing modules that incrementally introduce these issues as requirements for successfully completing the game. Player education will occur through sequentially increasing the requirements the player must satisfy in order to successfully complete the scenario. It is expected that the player will initially fail at meeting the requirements for successfully completing the game. As the player gains experience, through multiple game executions, and begins to comprehend, from instructor and game feedback, he will begin to master the fundamentals of confidentiality and appreciate the potential vulnerabilities introduced by his decisions.

1. Physical Security

Before discussing the aspects of physically security a definition must be provided as a basis for common understanding. In the context of this thesis Physical Security is:

> The application of physical barriers and control procedures to protect information and information systems. [ITSecurity 2004]

Providing physical security measures such as locks, safes, and guards is a fundamental requirement for protecting information. Some of these physical security measures, such as posting a guard, have been around for centuries, while more modern physical security measures, such as biometric authentication, have only recently been commercially available. Highly valued objects (e.g. cash, gold, information, etc…) have always required physical protection as a first line of defense and as the value of these objects to potential attackers rises, the amount of physical security required must rise as well. Fort Knox, home of the national gold reserve requires substantially more physical security than does the answer key to an exam. Thus physical security is essential to the success of any security plan, regardless of the object's relative value.

Physical security encompasses a range of measures that can be taken to protect information. These measure range from the extremely low tech mechanisms, such as locking valuable objects in a safe, to extremely high tech measures, such as requiring biometric authentication in order to gain access to an object. A minor oversight in physical security could be the Achilles heel of even the most elaborate and advanced high tech protection system. As Mies van der Rohe[2] once said, "the devil is in the details" and when it comes to security this is definitely true.

While physical security measures most often form the foundation upon which all other security measure can be built, they alone are not enough to protect objects. There is often a point at which the perceived value of the object is so high that physical security alone cannot protect the object. An example of this occurred in February 2003 when the Antwerp (Belgium) Diamond Centre was the site of the largest diamond heist in history. The robbers made off with an estimated $100 million in diamonds and left no clues as to how they did it.

[2] Mies van der Rohe is the German born American Architect (1886 –1969) most often attributed with this quote.

> The Diamond Centre at the heart of Antwerp's historic gem district has surveillance cameras everywhere and requires special passes to get in. The room where all the vaults are is even better protected, with round-the-clock guards standing by. [CNN 2003]

This elaborate, layered, and very expensive defense of the diamond vaults was overcome by a group of very determined and highly motivated thieves who had both the intelligence and patience required to identify the vulnerabilities in the physical security in place and exploit them.

Providing a basic understanding of the requirements and challenges associated with physical security is one of the main educational goals of this thesis. The scenario being developed will require that the player evaluate the physical security requirements needed to protect objects of differing values to attackers and then establish those measures deemed necessary to protect those objects from unauthorized access and theft. As a result the player will develop an understanding of the importance in establishing an appropriate level of physical security for ensuring the confidentiality of information.

2. Intranet

Intranets are essential for both commercial and military operations therefore a definition is provided to provide the reader with a basis of understanding. As defined earlier, an intranet is

> 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. [Webopedia 2004]

In the scenario developed for this thesis the intranet is the first network connection the player must deal with. Intranets are essential in today's commercial and military environment. They provide a high-speed, low cost means of communication amongst employees, they can provide a path for accessing an object (i.e. files, software, programs, etc…) located on a server or other storage medium, and they can provide an efficient means of providing information and guidance through the use of an intranet based web site.

A key aspect of an intranet is its separation from other networks. This separation can be either physical or logical. A physically separate intranet ensures that no external network access can be gained to the network. This provides for strong network security however it does not prevent internal attacks. Additionally, physical separation not only prevents outsiders from coming in, it also prevents insiders from getting out. While this may be acceptable in some highly secure military networks it is often not acceptable for commercial and routine military purposes. Therefore, the need for internal users to gain access to some external network requires that the intranet be logically separated by some technological means, such as a firewall. Firewalls are primarily used to logically separate an intranet from an external network. Firewalls can be configured to allow access by internal users out and to block external users from gaining internal access. This ability to physically connect an intranet to an external network while simultaneously keeping it logically separate is essential for contemporary business activities.

The scenario developed for this thesis requires the player to make decisions concerning which virtual users need access to the intranet and which do not. Players will also have to decide which assets (information) need to be accessible via an intranet. The basic security concept that this scenario demonstrates is that a connection to a network, even an internal network, may produce immediate and catastrophic vulnerabilities to valuable assets. To win this scenario the player will need to recognize the potential solutions and weigh the benefits and consequences of each in order to meet the virtual users' goals and complete the scenario.

3. Internet

The Internet is the largest interconnection of computers in the world. It spans the globe and can be accessed from virtually anywhere on the planet. It provides instant access to incalculable amounts of information and can be accessed by anyone with a networked device of some sort. As reported by the Computer Industry Almanac the estimated number of Internet users in 2004 is 945 million and expected to rise to 1.46 billion by 2007. [ClickZ 2004]

The ubiquitous and user-friendly nature of the Internet has revolutionized the concept of access to information. Business decisions and military planning alike are inextricably reliant upon instant and accurate access to information. Leaders, decision makers, and ordinary people no longer consider instant, reliable access to information as a luxury; they now consider it a necessity. This creates a dilemma when planning a security policy for protecting information. Decisions must be made that both protect information from unauthorized access while simultaneously providing access for authorized users via the Internet. While a highly secure military facility may be able to function in complete isolation, this is not true for today's commercial, and increasingly for today's military, endeavors. Thus connecting to the Internet is a double-edged sword that requires consideration of both its, risks and benefits.

In addition to granting internal users access to the Internet, access by external users must be considered. There are numerous situations where a remote user may require access, via the Internet, to an intranet. These situations include users on business travel who require access to a company-maintained database, students who need access to their school's intranet in order to complete assignments, or customers who require access to internal company networks to conduct business (e.g. Internet based bank account management).

In the scenario developed for this thesis, the player will be required to provide the virtual users in the game access to the Internet. In addition, there is a requirement to grant remote users access to a company-controlled web server. These requirements are intended to familiarize the player with some of the basic security issues and decisions necessary to fulfill user requirements for access to information while simultaneously protecting that information from unauthorized access. There are numerous decisions that the player will be able to make to meet these requirements, each of which has benefits and detriments. The primary educational goal is to illustrate to the player the importance of network configuration to the security of classified information and that there are often multiple solutions that fulfill the requirement.

C. SUMMARY

This chapter has provided the reader with an understanding of who the intended users, of the CyberCIEGE game, are and why. It also informs the reader of the differences between the roles (instructor or player) the game's intended users might fulfill. Finally, this chapter identifies and justifies the intended educational goals of the CyberCIEGE scenario that has been developed for this thesis. The following chapter will describe and provide details concerning the CyberCIEGE game that has been developed for this thesis.

IV. SCENARIO DESCRIPTION

A. SCENARIO OVERVIEW

This scenario was developed to answer the first question posed in this thesis, can a CyberCIEGE scenario be developed such that it is simultaneously a playable game and an educational tool that illustrates confidentiality issues in an internal corporate network connected to the Internet? To accomplish this the scenario was written to meet the educational goals delineated earlier in this thesis. This chapter will describe the scenario in detail and identify how each aspect of the scenario correlates to the educational goals identified earlier. Finally, since the security concepts being taught are fundamental to any Information Assurance program, the scenario written for this thesis is based in a corporate environment, however many of the lessons learned in it can translate directly to a military environment.

The scenario simulates the plight of *VentureGames* (VG). To begin business operations VG has acquired a small office building where it can set up its corporate offices. The offices are empty and no equipment or networks currently exist. Quickly establishing a functional office is paramount to the success of this scenario.

VG is in a very competitive industry and thus must protect their proprietary work and intellectual property. To conduct daily business the company needs a private internal network (Intranet) as well as connection to the Internet. Employees use the VG intranet to communicate with each other and to access databases and servers that contain information they require to meet their goals. The Internet is for external communications and research purposes. VG employee's happiness and productivity will be affected, both positively and negatively, by the ease at which they can meet their goals.

Although *VentureGames* is only a startup computer gaming company it is in the process of developing a Next Generation (NG) video game. This NG game is the most valuable asset that the company owns. Its successful development and production will make *VentureGames* a major player in the computer gaming industry. This NG game is so revolutionary that *VentureGames'* competition is determined to get a copy of it;

additionally the gamer community has gotten wind of the NG game and is very active in trying to obtain a pirated copy of it from the Internet.

The goal of the player will be to provide the components necessary for the company to establish both an internal network and a connection to the Internet so that the company employees can meet their goals. Ensuring the confidentiality of the company's classified information is the key to success in the scenario. However, establishing overly intrusive security measures will negatively affect the employee's productivity and happiness. Conversely, insufficient application of security measures will create vulnerabilities that potential attackers may take advantage of to compromise the classified information, which will have a catastrophic effect on the company's ability to operate.

The player will assume the role of *VentureGames'* new Information Technology Manager. The player will be provided with a budget and will be given one month to identify the requirements, purchase the components, and provide the connectivity that is required for the virtual users to meet their goals. If after one month the player has not been able to make a profit for the company, lost all his money, or if the NG Game Code is compromised, the player will lose. If the player instead makes choices that both provide protection for the NG game and enable the virtual users to meet their goals the player will win.

To accomplish the educational goals identified, the *VentureGames'* Scenario is played in five sequential modules each of which builds upon lessons learned in the previous module. The first module introduces the concept of physical security. To win this module, the player simply needs to provide adequate physical security to protect *VentureGames'* assets. Module Two introduces the need for an intranet in the company. The key to success in this module is to provide adequate physical security and to properly identify which virtual users require access to the intranet and which do not. The third module takes the intranet to the next level by requiring the player to provide intranet access to the virtual user who maintains the NG game code (*VentureGames'* most valuable asset). The key to success in this module is to provide sufficient physical security and then to choose between one of two acceptable means of providing the

required access. Either providing the virtual user with a separate component to gain access to the intranet or to physically connect the virtual user to the intranet but to logically separate them by using a firewall are satisfactory solutions. Both of these configurations have advantages and disadvantages that must be accounted for but each is winnable if the correct choices are made. The fourth module introduces the requirement of connecting to the Internet. One of the virtual users has a new goal of accessing a database located at a remote site. Once again, providing sufficient physical security and choosing one of two potentially successful network configurations will determine the player's success or failure. Finally the fifth module encompasses the concepts identified in the previous four and adds the requirement of an external virtual user gaining access to an internal *VentureGames'* component. This module is the capstone for this scenario; if the player learned the lessons from the previous module and applies them appropriately they will have successfully completed the *VentureGames'* CyberCIEGE scenario.

B. NARRATIVE

The narrative is provided as a means for explaining the goals and requirements of the player in the game. The narrative includes a briefing that welcomes the player to the game and a short description of the virtual users, their goals and the assets involved in the game. Additionally the parameters for success or failure are provided so that the player has a clear idea of what is needed to win the game. Finally, the narrative contains *Game Notes*, which can aid the player in making decisions, guide him through the scenario, and identify where he can look for help.

For this thesis, only the briefing for the final *VentureGames'* module (module 5) will be included, all other briefings are a subset of this briefing and therefore will be included in their modules' SDF as the appendices to this thesis. The following is the narrative provided in the fifth *VentureGames'* module:

Welcome to VentureGames! You have just landed your first big time IT job! It is with a small computer game development company called VentureGames (VG). VentureGames has just opened shop and you have been hired to set up and protect its IT infrastructure. The company has very little financial backing and minimal market share,

but they do have income from several successful games and the plans for a "Next Generation" game that, if successful, will catapult the company into the big time!

Your job is to design and maintain the company network, keeping the staff happy and productive while simultaneously ensuring the protection of the company's data. Good Luck! (See the "Game" tab for additional help)

Module five is an advanced game scenario. It is designed to challenge the player by demonstrating the difficulties associated with connecting an internal network to the Internet. This will illustrate some of the difficulties associated with granting external access to an internal network while protecting the confidentiality of sensitive information.

In this scenario there are five employees (users) that you need to help, Bob, Sally, Mark, Carl, and Paul. Additionally there are six assets that you need to protect: Employee Files, E-Mail, Marketing Plans, Legacy Code, NG Game Code, and the VG Web Site. Finally, there is an external user (customer) who wants access to a VentureGames' web site where he can gain information about the company and its games.

Bob is the founder and CEO of VentureGames (VG). Bob needs to access the employee files. These files are where Bob maintains the employees' records and evaluations. The records contain both employee personal and financial information, while the evaluations are used to determine which employees get raises, bonuses, advancement, and potentially dismissal. The information in these files is considered sensitive (VG PROPRIETARY) since its unauthorized disclosure could cause internal discord among employees.

Paul is the lead programmer at VG. He is in charge of developing the NG game code. Paul needs access to the NG game code. The code has the highest company classification (SIERRA) because its unauthorized disclosure could result in the financial ruin of the company. VentureGames' competitors would love to get their hands on this new code! Paul would like to limit access to the NG game code during its development.

Carl is a VG programmer. He is responsible for maintaining all of the legacy games owned by VG. These games, while not revolutionary, represent the primary

source of income for the company. Carl's primary mission is to keep the legacy game's customers happy by providing updates, fixing bugs, and providing expansion packs in an effort to extend the lifespan of these games. Since Carl has limited game development experience and is relatively new to the company he has not been granted access to the NG game code.

Mark is the company secretary. He answers the phones and greets visitors. His primary job is to maintain the employee files. He is responsible for the actual updating, recording, and maintenance of these files. He works directly for Bob but interacts with all VG employees. He has no technical computer experience and no comprehension of Information Assurance or Network Security.

Sally is the VP of Marketing for VentureGames. She is in charge of marketing all the VG games. Her current focus is on developing consumer demand for the NG game currently in development. Sally is a great marketing person, however she is not very computer savvy and often consumes a great deal of the IT department's time with routine and mundane problems that she can not fix. Sally's main goal is to develop the Marketing Plan for the NG game. This marketing plan contains VG PROPRIETARY information that if disclosed could be detrimental to the success of the company.

This scenario introduces the concept of an outside user needing access to the VG-internal network. In this scenario the customer wants to access the company's web site to gather information about the games provided by the company. You will need to provide this service for the customer when requested.

The assets that you need to provide access to and protect are the NG Game Code, Employee Files, E-MAIL, Marketing Plans and Legacy Code.

The NG Game Code is the MOST important asset the company owns and is therefore classified SIERRA. It has a very high value (300) to potential attackers. The value of this asset must be kept in mind when establishing security policies, access rights and network connectivity.

The Employee Files contain sensitive information that only the company management should see and are classified as VG PROPRIETARY. Keep this in mind when establishing security policies, access rights and network connectivity.

The E-MAIL is the primary means of communications amongst employees. Without it your company productivity will take a major hit. E-MAIL is classified NON-SENSITIVE.

The Marketing Plans are for the NG Game Code. They contain information concerning what the new game is and how it functions. This plans are classified VG PROPRIETARY and must be protected from external disclosure.

The Legacy Code consists of all the games that VentureGames currently offers and are classified as VG PROPRETARY. These games are relatively popular and provide the bulk of the company's income. These valuable assets must be protected in order to maintain this constant income flow.

There are three clearance levels in this scenario: SIERRA, VG PROPRIETARY, and NON-SENSITIVE.

SIERRA is the highest classification at VentureGames. It is reserved for use on only the most valuable of information. Disclosure of SIERRA classified information poses an extreme risk to the financial success and continued operation of the company. Employees are required to have a HIGH background check prior to receiving a SIERRA clearance.

VG PROPRIETARY classification is reserved for information that, if disclosed, could pose a serious risk to the financial success and continued operation of the company. A MEDIUM level background check is required for an employee to receive a VG PROPRIETARY clearance.

NON-SENSITIVE classification includes all publicly releasable data. This information poses no risk to the company. There is no background check required for a NON-SENSITIVE clearance.

To win this game, you must make a profit for the company. To do this, you will need to provide the IT support necessary for the users to reach their goals and the

security measures necessary to protect classified assets. If the NG Game Code is compromised by your competitors (an external attacker) you will immediately lose! Internal disclosures and Denial of Service (DoS) attacks, both external and self-imposed, will result in financial loss.

GOOD LUCK!!

GAME NOTE: Set up your IT infrastructure prior to going operational (i.e. UNPAUASE).

GAME NOTE: Get familiar with the users, their goals, the assets, and the zones in the game prior to going operational (i.e. UNPAUSE).

GAME NOTE: Check the access list for each zone and component to ensure that the Principle of Least Privilege is enforced.

GAME NOTE: Hit the "e" key to access the game's encyclopedia.

C. ACCESS CONTROL POLICIES

There are two types of Access Control Policies that will be used in the *VentureGames'* scenario. These two policies are Mandatory Access Control (MAC) and Discretionary Access Control (DAC). A formal definition of each is provided to aid the reader in understanding what each of these access control policies means and its implications to the game.

A Mandatory Access Control Policy is formally defined as a:

> Means of restricting access to objects based on the sensitivity of the information contained and the formal authorizations (i.e., clearance, formal access, approvals, and need-to-know) of subjects to access information of such sensitivity. [CNSS 2003]

A Discretionary Access Control policy is formally defined as a:

> Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (directly or indirectly) to any other subject. [CNSS 2003]

The key difference in these two access control policies is that in a DAC policy subjects (users, programs) can change the access permissions to objects while in a MAC policy subjects cannot change these permissions. In a MAC enforcing system the policy is enforced by the system and can only be changed by an administrator in a DAC system the users can change the access policies as they please.

VentureGames has established the following access control policies. These policies are key aspects to the game. They provide both the motivation for the player to protect the assets and for the attackers to gain access to them. The mandatory policies are enforced by the game's components while the discretionary policies can be established or changed by the player during the course of the game.

1. Mandatory Policies

The following classifications are currently in effect at *VentureGames*. All of the *VentureGames'* assets have been assigned one of these classifications to create a value for that asset which the player must protect and an attacker is motivated to obtain. The game engine will enforce the Mandatory Access Control policy to enforce the protection of assets having these classifications. For example, the player will not be able to access or create an asset with *SIERRA* classification on a system that is only authorized to hold up to *VG PROPRIETARY*.

SIERRA - *This is the highest classification at VentureGames. It is limited to use on assets that, if they were to be compromised, would financially ruin the company. Users must have a high background check to receive this clearance.*

VentureGames is currently in the developmental stages of a "Next Generation" video game. This NG game, if successfully launched, will dominate the industry and establish VentureGames as a major player in the gaming industry. The game, and the information concerning it, is the most valuable assets owned by the company. The NG game is an advanced, 3-D, first person, networked action/adventure game. The graphics, sounds, and animations are revolutionary in their design and implementation and its cross-platform capability will make it executable on every flavor of gaming system. If

information regarding the specifications, concepts, algorithms, or high-level design details of this game are compromised VentureGames' future prospects as a company will be devastated. VentureGames' competitors already hold significant financial, production, development, and marketing advantages over them. If they obtained this information without having to incur the considerable expense required to resolve the technical issues associated with this "Next Generation" technology they would easily overcome VentureGames in the development of this new type of game. Only users cleared to SIERRA should have access to this data.

This clearance has a secrecy value of 5000 and has an attacker value of 300. Disclosure of this information poses an extreme risk to the financial success and continued operation of the company.

***VG PROPRIETARY** - This classification is reserved for use on assets that require protection but whose compromise, while still serious, would not be devastating to the company. Users must possess a medium level background check to receive this clearance.*

The NG game's high level marketing plans and concepts as well as their ongoing developmental status is information that would cause serious damage to VentureGames' if known by its competitors. In addition the company needs to protect its legacy game software and detailed designs. Only users having a VG PROPRIETARY clearance should have access to this data.

Users having SIERRA clearance implicitly are cleared to access this data. This clearance has a secrecy value of 500 and has an attacker value of 50. Disclosure of this information poses a serious risk to the financial success and continued operation of the company.

***NON-SENSITIVE** – This is the lowest classification at VentureGames. Users do not require a background check to receive this clearance.*

This is publicly available information such as released marketing material, corporate information, and other openly published information. This clearance has a

secrecy value of 0 and an attacker value of 0. Disclosure of this type of information poses no risk to the company.

2. Discretionary Policies

The following discretionary access groups have been established for the *VentureGames'* scenario to enhance the game's playability and entertainment value. By introducing interests, among the *VentureGames'* employees, that conflict with the security policies established in the game, the player is introduced to some of the challenges in enforcing such policies.

PROGRAMMERS *- The members of this group are the programmers who develop and maintain the games (NG game as well as legacy games). This DAC group has been created to keep non- programmers from accessing the code, legacy and NG.*

The programmers have been hearing rumors that once the NG game is completed and ready for distribution the company is going to end support for the legacy games and layoff some programmers. Some of the programmers have been intentionally falling behind schedule and/or sabotaging the development of the NG game in order to keep their jobs. The programmers are trying to keep management from finding out how far behind schedule the programmers are.

MANAGEMENT *- These group members encompass the management staff of the company. They make the decisions that guide the company. They have final say in the development, design, production, and marketing of the games. They are also responsible for securing the necessary finances needed to fund the company's operation, research, and development. Management created this DAC group to keep sensitive managerial information protected from internal users gaining unauthorized access.*

It is imperative that management prevents the rest of the company's employees from finding out that VentureGames is in serious financial trouble. The existence of the company is intertwined with the successful and on time release of the NG game. Any

delays in its development or release will be financially devastating to the company. In addition management has decided to end support of the legacy games once the NG game is launched, therefore they have developed a plan to layoff some employees. Management must ensure that no unauthorized personnel ever see this plan.

***COMPANY** – Everyone who works for VentureGames and requires access to components or the network is in this group. This group includes the IT staff and other everyday employees. Being a member of the company group differentiates employees of the company from the general public. VentureGames' facility has many valuable assets in it, both physical and intellectual, and these assets must be protected. Access by non-company personnel should be limited to the absolute minimum.*

***PUBLIC** – By default, all users in the CyberCIEGE game belong to the PUBLIC group. This group also contains VentureGames' competition, and both script kiddies and hackers residing on the Internet that want to gain access to or modify VentureGames' assets. Access to VentureGames' assets by the public must be limited to the VG Web Site to prevent unauthorized access to classified information.*

D. ASSETS

Assets are an essential element to the game. They are what the virtual users need, or want to gain access to, in order to be productive and happy in the game. These assets are conceptual in nature in that they must first be instantiated on a component for the virtual users to reach their asset goals. Figuring out how to provide the virtual users access to their assets while simultaneously preventing any unauthorized access to these assets is the fundamental educational goal in this scenario.

Assets can come in the form of intellectual property, such as game code, or in physical form, such as a database. Additionally the assets have varying degrees of value to the enterprise. Some may be extremely valuable while others are not valuable at all. The value of an asset may be due to its classification (e.g. SIERRA, MANAGEMENT)

or it may be due to its integrity (integrity is not the focus of this scenario). Either way these assets must be protected from attacks.

Each asset has a varying degree of value to an attacker. The higher the asset's attacker value or motivation (ranging from 0 to 1000) the more likely it is to be compromised. Each asset has two values that determine its value or motivation to a potential attacker. The first is determined by the attacker value identified in the MAC clearance assigned to the asset. The second is determined by the attacker motivation to break the DAC policy assigned to the asset. These two distinct attacker-motivating values provide the impetuous for both internal and external attacks against a classified asset. By adjusting these values the scenario developer can introduce game intrigue, complexity, and realistic simulated game play. Additionally the scenario developer can adjust these values to tune the scenario to an appropriate difficulty level for the intended player thus providing tailored training to the player.

The following table delineates the relationship between the numerical attacker value or motivation and a real world equivalent of the potential attacker's skill and degree of motivation:

Attacker Value/motive	**Degree of attacker motivation/skill**
0	No value to an attacker. No protective measures required.
25	Valuable to amateur hackers (script kiddies) with interest in low-level vandalism. Requires limited protective measures.
50	Valuable to hackers with moderate interest in gaining access or vandalizing and who have advanced skills. Requires robust protective measures
100	Valuable to Crackers (professional hackers) with financial interests and extensive expertise in gaining access. Requires extensive, layered protective measures.

1000	Nation state with national interests and unlimited resources to gain access. Virtually impossible to protect against.

Table 1. Attacker Values

To successfully complete the scenario the player must identify the appropriate level of security required to protect each asset while simultaneously providing an appropriate means of access to each asset for the virtual users. This balancing act, security versus access, which the player must perform, is a key concept in the protection of classified information being demonstrated by the *VentureGames'* scenario.

The following assets are included in the *VentureGames'* CyberCIEGE scenario:

Next Generation Game Code - *This is the Next Generation (NG) game code. Its successful development is critical to the financial success of the company. The company's competitors and computer game enthusiasts are both interested in gaining access to this code.*

This is the most valuable asset the company owns and is therefore classified SIERRA. Its successful development is critical to the company's ability to operate in the future; any unauthorized access or delays in production will have a catastrophic effect on the company. In addition to requiring protection form external unauthorized access, this asset must be protected from internal unauthorized access.

The development of this game code is very far behind schedule. The user responsible for its development wants to ensure that no one finds out how far behind he is on the code. Therefore only he should have access to this asset.

Legacy Code - *The Legacy Code includes all the games that VentureGames currently owns and maintains. These games are moderately popular and are currently the sole source of income for the company.*

While these games are currently on the market their actual game code still requires protection and is therefore classified VG PROPRIETARY. Game enthusiasts, script kiddies, and hackers alike continually attempt to steal this asset in attempt to get the games for free. Compromise of this asset will result in financial difficulties for the company.

The programmers have spent countless hours on the development of the VG game library. They would prefer that the bare minimum number of people, to include management, be able to gain access to the code.

***Marketing Plans -** These are the Marketing Plans for the NG game. They contain proprietary information concerning the game and its revolutionary "game play".*

The marketing plans contain details concerning the NG game and its revolutionary game play, as well as all of VentureGames' market and research data that has been collected to develop an advertising campaign to garner interest in the NG game. Since VentureGames' competitors are interested in gaining advanced copies of these plans, this asset is classified VG PROPRIETARY.

Management wants to limit access to the marketing plans until the NG game is ready for release. The marketing plans contain information that, if compromised, could provide an undue advantage to the competition, which will cause serious financial damage to the company.

***Employee Files -** These are the files that contain the VentureGames' employee information. This information includes sensitive personal and financial information as well as classified employee evaluations, promotion lists, and layoff schedules. Management wants to protect these files from unauthorized access. Since these files contain personal employee information, such as pay amounts and employee evaluations, as well as management's plans to layoff some employees after the NG game has been completed, they have been classified VG PROPRIETARY.*

The rest of the company's employees have great interest in seeing these files especially the programmers who face potential layoffs. Only management should gain access to this asset.

E-MAIL *- E-mail provides a means of communications amongst employees and, if connected to the Internet, with people outside of the company. It is provided as a means to conduct company business, however it is used often for personal correspondence as well.*

General company e-mail is not considered to be sensitive and is, therefore, classified Non-Sensitive. Its compromise presents little risk to the company.

Although company e-mail is not classified VentureGames' management would prefer that only company employees gain access to it.

VG Web *- This is the VentureGames' web site. It provides information about games being developed, company contact information, and links to download free game versions, patches, and updates. It is the face of the company to its customers.*

The information on this asset has been cleared for public release and poses no threat to the company. However if it is vandalized or defaced it could harm the company's reputation.

The web site should be read accessible by the general public as well as the VentureGames' employees but should not be written to or modified by unauthorized users.

Marketing Research *- Marketing Research is used to determine consumer demand and trends. It is provided by a national marketing association and is a database containing current consumer trends such as, consumer likes and dislikes, age group, ethnic, and gender based purchasing patterns, and consumer preferences. This national*

database is essential for small marketing firms and independent marketers for getting the latest and most accurate marketing data available.

This asset is for public use and is maintained and supported by a remote site (not belonging to VentureGames). It posses no threat to the company and has a Non-Sensitive classification. This asset should be accessible by the general public.

E. ASSET GOALS

Key aspects of the assets are the goals the virtual users have concerning accessing those assets. Each asset goal has an asset associated with it. These asset goals are assigned to the virtual users and determine their goals in the game. Virtual users can have a single or multiple asset goals. The asset goals can all be instantiated at the outset of the game, so that the player can meet them all early in the scenario, or they can be instantiated during the game play, to provide variety to the game scenario or stress on the player to meet new goals that may conflict with previously made decisions. This flexibility provides the game scenario designer with the ability to model the changing real world demands that IT personnel face.

The following are the descriptions of each of the asset goals included in the *VentureGames'* scenario:

Write NG Game Code *- The goal is to be able to access the NG Game Code and modify it as necessary. The NG Game Code requires a word processing program to access it.*

Maintain Legacy Code *- The goal is to be able to access the Legacy Code in order to maintain it. The Legacy Code requires a word processing program to access it.*

Access Employee Files *- The goal is to be able to access the employee files so that they can be updated and reviewed. The Employee files require a Word Processing program and management program to access them.*

Develop Marketing Plan *- The goal is to be able to access the Marketing Plan so that they can be updated and reviewed. The Marketing Plans require a Word Processing program to access them.*

Access E-MAIL *- The goal is to be able to access E-MAIL so that users can send and receive correspondence. To access E-MAIL an E-MAIL Client and server are required.*

Research Marketing Data *- The goal is to be able to access the online Marketing Research database. In order to access the Marketing Research data, a web browser is required.*

Access Web Site *- The goal is to be able to access the VentureGames' Web Site in order to gather information about games currently being developed, get company information, download patches and/or updates to games, and to download free games and/or other content provided by the company.*

F. VIRTUAL USERS

Virtual users are the simulated agents, typically employees, within each scenario who interact within the virtual environment and are affected by the decision made by the player. Virtual user's happiness and productivity, which are determined by their ability to meet their goals, contribute to the financial success of the enterprise. Unhappy and unproductive virtual users are not only a detriment to the financial success of the enterprise; they are also a detriment to the protection of classified information.

Several aspects of the virtual user are established within the Scenario Definition file. These aspects include the virtual user's name, job description, discretionary access groups, mandatory clearances, trustworthiness, asset goals, training, happiness, and productivity. Each of these virtual user aspects is defined in detail in the CyberCIEGE encyclopedia, which is included in the game.

In addition to the virtual users, who act as the company's employees, the Scenario Definition File allows for the creation of an enterprise support staff. These agents make up both the IT support personnel and the security guard detail that can be employed within the scenario. These support agents are different from the virtual users in that the player can hire and fire them at will, and in that their salaries come out of the player's IT budget, where as the enterprise's virtual users' salaries do not. The goal of the player is to facilitate the company employees' ability to meet their asset goals. This is accomplished through the procurement of components, establishment of networks, and providing the appropriate support personnel necessary to ensure its availability and security.

1. Employees

The following is a description of the virtual users that make up the employees in the *VentureGames'* CyberCIEGE scenario. These users are instantiated at the outset of the game and cannot be hired or fired by the player. Their productivity, happiness, and ability to reach their goals will affect the finances of the company in either a positive or negative way. To successfully complete the scenario the player must make decisions that facilitate these users in accomplishing their goals while protecting the assets from unauthorized access.

Paul *- Paul is the lead programmer and project manager for the NG game. Its development is his only task. He is a phenomenal programmer, can code anything, loves what he does and works hard. Gets very upset very fast if he can't access his stuff because of "network" problems. An "Open Source" advocate, he hates to use proprietary software. He knows about network security but doesn't always practice it. He is highly trustworthy, and can be counted on to be very productive. Paul holds a SIERRA level clearance and belongs to the Programmer, Company, and Public DAC groups.*

His main goal in the game is to develop the NG game code. A secondary goal Paul has is to access his email account. To be productive and happy, Paul needs access

to the NG game code all the time, while his access to his e-mail is only required after he requests it. Paul needs access to productivity software to do his job. If he does not have this access it will negatively affect his productivity and happiness. Paul would prefer to have access to the game code and his e-mail from a single workstation, however if Paul can only access these assets on separate machines his productivity and happiness will only suffer a minor negative impact.

Carl – *Carl is a new programmer at VentureGames. He has been hired to maintain the legacy code so that Paul can focus on the NG game code. He is a recent Graduate from the University for the Super Smart. He is from the MTV generation and not only knows programming but networks too (he may have even done some hacking before). He likes his new job but only sees it as a rung on his ladder to success. Carl holds a VG PROPRIETARY level clearance and belongs to the Programmer, Company, and Public DAC groups.*

His main goal in the game is to maintain the legacy game code. Carl's secondary goal is to access his email account. To be productive and happy, Carl needs access to both the NG game code and his e-mail account at all times. Carl needs access to productivity software to do his job. If he does not have this access it will negatively affect his productivity and happiness, however his happiness will be more affected by an inability to access his e-mail than accessing the legacy code. Carl would prefer to have access to the game code and his e-mail from a single workstation, however if he can only access these assets on separate machines his productivity and happiness will only be affected slightly

Bob - *Bob is the founder of the company. He is an expert programmer, easily as good if not better than Paul. Bob and Paul are best friends. Bob is determined to get this company into the big time. Bob hired YOU! Much like Paul, Bob knows a great deal about programming but isn't a big "networks" guy. He knows all the security issues but is prone to overlook them if they are hindering the company's goal of writing code. Bob has hired you to deal with all these issues and is very supportive but does not always*

follow through with actions. Bob thinks programmers are great and network guys just weren't smart enough to be programmers! Bob holds a SIERRA level clearance and belongs to the Management, Company, and Public DAC groups.

His main goal is to access the employee files and read his e-mail. Bob needs access to productivity software to do his job. To be productive and happy, Bob needs access to these assets from one machine and at all times. If Bob has to use separate machines to reach his goals it will not affect significantly his productivity but will cause him to become very unhappy.

***Mark -** Mark handles the office. He maintains the company's administrative files. He also answers the phones and greets visitors. He is not technically savvy. Mark likes to talk and is very personable. He has no clue how a network operates or what it means to be secure, he does however love to get and send e-mail and download cool things for his desktop. Mark holds a VG PROPRIETARY level clearance and belongs to the Management, Company, and Public DAC groups.*

His goals are to access the employee files and read & write e-mail. Mark needs access to productivity software to do his job. Mark wants access to these assets at all times. If he can't access the employee files his productivity will take a hit. If he cannot access his e-mail his happiness will be negatively affected.

***Sally -** Sally's job is to build demand for the NG game. She wants to build a buzz about it to garner interest from the gaming public. She is not computer savvy at all, but a great marketing person. She wastes a lot of IT personnel time with routine and mundane problems. She often forgets passwords, leaves herself logged in, and habitually tries to download "cute stuff" for her computer. Sally holds a VG PROPRIETARY level clearance and belongs to the Management, Company, and Public DAC groups.*

Her primary goal is to develop the marketing plan. To do this Sally will require access to the Internet so that she can conduct market research on a database at a remote site. An additional goal for Sally is to access her e-mail account. To meet each of her goals, she

requires access to productivity software. For Sally to be both productive and happy, she needs access to these assets at all times and from one machine, if not her productivity and happiness will suffer a major negative impact.

2. External Users

The following user is a static user in the game. He is not an employee of *VentureGames* and therefore cannot be hired, fired or modified by the player. The customer only appears in the final module (module 5) of this scenario.

Customer – *Customer represents the external customers of VentureGames. His goal is to gain access to the VentureGames' web site. Customers can be good-natured and simply want information concerning the company, its currently available games, or games it has in production or they can have more devious intentions in mind. The player does not know what these intentions are, however to be successful in the game the player must provide the access necessary for the customer to meet his stated goal while simultaneously protecting VentureGames' assets against the customer gaining any more access than is required. Customer holds a Non-Sensitive clearance and belongs to the Public DAC group.*

3. IT Staff

Included in the game are a group of virtual users that can be hired or fired by the player. These virtual users make up the support staff. The player can choose to hire IT professionals to maintain and update the network and components, to hire security guards to increase physical security for the entire office or simply in one zone, or to hire both. The following are brief descriptions of each virtual user; more detailed information on each is available in the SDF.

The following are the potential IT employees the player can hire to ensure availability and maintenance of the components and network:

Dan – *Dan is an experienced IT professional but does not have a college degree. He is a hard worker but sometimes has an attitude if he thinks people look down at him for not having a degree. Dan is extremely trustworthy and competent in his job but is prone to complaining. He can be hired at a salary of $1300 per month. Dan holds a Non-Sensitive clearance and belongs to the Company and Public DAC groups.*

Warren – *Warren graduated with honors with a degree in Computer Science and is certified in several areas but he lacks actual work experience. He is trustworthy and is very well trained. He is a very positive person and gets along with people very well. He can be hired for $1400 per month. He holds a Non-Sensitive clearance and belongs to the Company and Public DAC groups.*

J.D.– *J.D. has over 20 years of IT experience. He is an expert in both software and hardware. He has numerous certifications in network and IA security. J.D. is the consummate professional, knows his job, gets along with people and is a positive influence on his fellow employees. He can be hired for $1500 per month. He holds a Non-Sensitive clearance and belongs to the Company and Public DAC groups.*

4. Security Guards

The following are the potential security employees the player can hire to ensure the physical protection of the company's valuable assets:

Klaus – *Klaus is very good with people and a hard worker but he tends to not do his job if distracted. He is trustworthy and competent at his job. He can be hired for $1200 per month. He holds a Non-Sensitive clearance and belongs to the Public DAC group.*

Axel – *Axel is very strict and disciplined. He is very trustworthy but often rubs people the wrong way. He is an expert in the field of security. He can be hired for $1300 per month. He holds a Non-Sensitive clearance and belongs to the Public DAC group.*

Hans – *Hans is a good security guard and gets along well with the staff. He is very trustworthy and is a productive employee. He can be hired for $1200 per month. He holds a Non-Sensitive clearance and belongs to the Public DAC group.*

G. SUMMARY

This chapter has provided a description of the *VentureGames'* CyberCIEGE scenario and the key aspects of it. The policies, assets, asset goals, and virtual users that make up the game have been introduced and a brief description provided. Additional details concerning these aspects, as well as issues concerning game play, are more thoroughly addressed in the CyberCIEGE encyclopedia.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TESTING

A. TEST STRATEGY

The CyberCIEGE game engine is complex and non-deterministic in nature and therefore it is difficult to predict its exact behavior when executing a scenario definition file. In addition, the development of the scenario definition files themselves is a very complex task, which affords ample opportunity for errors to be introduced, that can affect the game engine's performance. Therefore, the strategy chosen to test the game engine's performance was to develop a small set of test cases, which model a specific aspect of security, and predict the outcome of these test cases. From these initial test cases, more complex test cases were incrementally developed. The results of these test cases were collected and weighed against the results that were predicted prior to executing the game. The culminating outcome of these test cases verifies that the game engine is able to accept a customized SDF and execute a game simulation that models the real world in an acceptable manner.

The testing approach used for validating the CyberCIEGE game engine's performance is the Verification Validation and Accreditation (VV&A) [DMSO2 2003] process. Specifically, the face validation process of VV&A was utilized in the testing phase of this thesis. Face validations is defined as:

> The process of determining whether a model or simulation seems reasonable to people who are knowledgeable about the system under study, based on performance. This process does not review the software code or logic, but rather reviews the inputs and outputs to ensure that they appear realistic or representative. [DOD 1997]

The CyberCIEGE game engine has two key aspects regarding its verification that lend itself to the face validation process. First, it is nondeterministic in nature, i.e. a specific action or setting is expected to occur with a certain probability rather than as a direct function. Second, the resultant outcome of an action cannot be measured by quantitative means, it must be examined using qualitative measures to determine its acceptance or not.

In the face validation process designed for this thesis the developer of the SDF acted as the subject matter expert for the test. This facilitated both the development of the test SDFs for game engine validation and the playable game scenario SDFs, while keeping the test phase of the thesis within the scope of the thesis schedule. Additionally, this approach to testing the game engine provided numerous test cases that can later be incorporated into a high level, overall test strategy.

Finally, it is important to identify that the test phase for this thesis occurred while the game engine was still being adjusted and modified to meet the CyberCIEGE project's specifications. This was also the case for the Scenario Template Format (SFT), which is the document that identifies the games parameters and settings. Therefore, the test cases in the following chapter have been tested on more than one version of the game engine.

B. TEST CASES

This section identifies and describes the most significant test cases conducted during the test phase. Each of the following test cases is laid out in a similar three-tiered format. The first section describes the test case, defines the scope of the test case, and references the educational goal it relates to. The second section defines the results the test case developer expects to occur during the game's simulation. Finally, the third section identifies the actual results of the game simulation.

The test cases were developed in incremental steps, from simple to complex, in order to limit errors caused by poorly constructed scenario definition files. Each test case has multiple testing variations, such as high physical security or low attacker motives. These variations are needed to ensure that the game engine properly identifies and simulates the numerous variables that compose the realm of Information Assurance and Network Security.

1. Test Case 1 "Physical Security"

a. Test Goal and Design

Physical security is a fundamental security measure in protecting information. In this test case the concept of physical security is introduced and modeled.

The goal of this test case was to identify whether the game engine modeled the basic issues involved with protecting classified information by physical security means alone in an acceptable manner. Additionally, it identified some basic security measures that can be utilized to provide security for confidential information.

In this test case, there is one user, Paul, who has an asset goal of writing the Next Generation (NG) Game Code. This asset, NG Game Code, has been instantiated on Paul's workstation, which is located in a walled office that has access control established in the form of various physical security measures, i.e. a cipher lock on the door. Paul's computer is not connected to any networks and only Paul has permissions to access this asset.

To conduct this test case the attacker motivation and the degree of physical security provided were adjusted, i.e. high attacker motivation and low physical security, in each execution of the test case. All other aspects of the test case remained constant through each subsequent execution of the test case. These permutations, of the test case, were essential for validating that the game engine properly recognized the differing degrees of motivation and protection possible in the real world, and model a realistic outcome. The following list identifies the title of each physical security test case conducted and its attacker motive and physical security settings:

- VGTest1a_PhysSecurity_Sec-low_Mot-low.sdf
- VGTest1b_PhysSecurity_Sec-low_Mot-med.sdf
- VGTest1c_PhysSecurity_Sec-low_Mot-high.sdf
- VGTest1d_PhysSecurity_Sec-med_Mot-low.sdf
- VGTest1e_PhysSecurity_Sec-med_Mot-med.sdf
- VGTest1f_PhysSecurity_Sec-med_Mot-high.sdf
- VGTest1g_PhysSecurity_Sec-high_Mot-low.sdf
- VGTest1h_PhysSecurity_Sec-high_Mot-med.sdf
- VGTest1i_PhysSecurity_Sec-high_Mot-high.sdf

b. Expected Results

Each of the individual test scenarios for the physical security test case should produce slightly different results. Since all aspects of the test, except the attacker

motivation and the degree of physical protection utilized to protect a classified asset, remain constant any variations in the test case outcomes can be attributed to the chosen test variables. The following table delineates each test scenario with the test designer's expected pre-test execution results.

Test ID	Physical Security Whole Office	Physical Security Paul's Office	Attacker Motivation	Expected Results
VGTest1a.	0	9	100	Paul will have access to the asset but it will be compromised and his workstation will eventually be stolen.
VGTest1b.	0	9	400	Paul will have access to the asset but it will be compromised and his workstation will eventually be stolen.
VGTest1c.	0	9	800	Paul will have access to the asset but it will be compromised and his workstation will eventually be stolen.
VGTest1d.	182	203	100	Paul will have access to the asset and it will not be compromised. His workstation will not be stolen.
VGTest1e.	182	203	400	Paul will have access to the asset but it will be compromised. His workstation will not be stolen.
VGTest1f.	182	203	800	Paul will have access to the asset but it will be compromised. His workstation will not be stolen.
VGTest1g.	357	394	100	Paul will have access to the asset and it will not be compromised. His workstation will not be stolen.
VGTest1h.	357	394	400	Paul will have access to the asset and it will not be compromised. His workstation will not be stolen.
VGTest1i.	357	394	800	Paul will have access to the asset but it will eventually be compromised due to the high attacker motivation. His workstation will not be stolen.

Table 2. VGTest1 Expected Results

c. Actual Results

The test scenarios were developed and executed while the CyberCIEGE game engine was still being updated, modified, and refined. Therefore, each test scenario was executed using the same version of the game engine to ensure that no anomalies resulted due to the differences in the game engines. During the execution of the test case the results produced by each of the test scenarios were observed, during the test's execution, to determine if the game simulation was realistic. Once the game concluded the game results were then inspected through the use of the scenario's *results file*[3] and *log file*,[4] which are provided by the game engine. These results were then compared to the results the test designer expected prior to the game's execution.

The following table presents the actual results and identifies whether they met the designer's expectations.

Test ID	Actual Results	Met Expectations
VGTest1a.	The test case met expected results. Paul was a happy and productive worker while he had access to his workstation and the asset. The asset was disclosed almost immediately. Both MAC and DAC attacks occurred and the workstation was eventually stolen. Once Paul's workstation was stolen, his productivity and happiness dramatically decreased.	Yes
VGTest1b.	The test case met expected results. Paul was a happy and productive worker while he had access to his workstation and the asset. The asset was disclosed almost immediately. Both MAC and DAC attacks occurred and the workstation was eventually stolen. Once Paul's workstation was stolen, his productivity and happiness dramatically decreased.	Yes
VGTest1c.	The test case met expected results. Paul was a happy and productive worker while he had access to his workstation and the asset. The asset was disclosed almost immediately. Both MAC and DAC attacks occurred and the workstation was eventually stolen. Once Paul's workstation was stolen, his productivity and happiness	Yes

[3] The game engine creates a results file during the game. It annotates the key aspects of the game's activity such as which attacks occurred and why they occurred.

[4] The log file captures all game activity to include the scenario's setup and creation. This file aids in identifying errors that cause unintended results.

	dramatically decreased.	
VGTest1d.	Paul remained a happy and productive worker for the duration of the test (1 month). Paul's workstation was never stolen and remained available to him. The asset was not disclosed.	Yes
VGTest1e.	Paul remained a happy and productive worker for the duration of the test (1 month). Paul's workstation was never stolen and remained available to him. An external attacker disclosed the asset.	Yes
VGTest1f.	Paul remained a happy and productive worker for the duration of the test (1 month). Paul's workstation was never stolen and remained available to him. An external attacker disclosed the asset.	Yes
VGTest1g.	Paul was a productive and happy worker, but did not like all the security requirements imposed on him. The asset was not disclosed and the workstation was not stolen.	Yes
VGTest1h.	Paul was a productive and happy worker, but did not like all the security requirements imposed on him. The asset was not disclosed and the workstation was not stolen.	Yes
VGTest1i.	Paul was a productive and happy worker, but did not like all the security requirements imposed on him. The asset was eventually disclosed but the workstation was not stolen.	Yes

Table 3. VGTest1 Actual Results

The results of these test scenarios met the test designer's expectations. The asset, if left unprotected, was either quickly disclosed or the workstation containing it was stolen. Increasing the amount of physical security allowed the asset to be protected and increased the amount of attacker motivation required to compromise the asset or steal the workstation. The final test scenario, high physical security and high attacker motivation, demonstrated the inherent failings of providing physical security alone and highlighted the need for additional protective measures, i.e. password protection and access controls, for protecting high value, confidential assets.

2. Test Case 2 "Intranet"

a. Test Goal and Design

Test Case 2 introduces two new users to the game. First there is Mark, the company secretary. Mark is an un-trusted user and holds a low security clearance. He

works in the main office and handles the personnel files of the company on his workstation. Since these personnel files are classified Non-Sensitive, Mark's workstation does not have any physical protection; it sits on his desk in the open office.

The second new user is Sally. Sally is in charge of marketing *VentureGames'* products. Her marketing plans are classified *VG PROPRIETARY* and must be protected from unauthorized disclosure. Sally's classified marketing plans are located in her office; therefore, her office has high (935) physical security, i.e. cipher locks, guards, and alarms, established to protect it. The rest of the office has low physical security (52) established to protect against theft only. Additionally, in this test case there is a newly installed *VentureGames'* intranet that its employees can connect to.

The high value asset that requires protection, in this test case, is the VG marketing plan located in Sally's office. Since this office has high (935) physical security established compromise of the asset through physical means is highly unlikely, thereby making the intranet connection the most likely vulnerability to the high value asset. Therefore, the goal of this test case was to identify whether the game engine modeled the issues involved with protecting classified information, residing on a workstation, connected to an intranet in an acceptable manner. This included validating that the game engine properly modeled firewalls and their filters. The following list identifies the title of each intranet test scenario conducted:

- VGTest2a_Conf_Intranet_No_Access.sdf
- VGTest2b_Conf_Intranet_No_Firewall.sdf
- VGTest2c_Conf_Intranet_Firewall_BlockAll.sdf
- VGTest2d_Conf_Intranet_Firewall_BlockAll_In.sdf

b. Expected Results

In general, the expected results of these test cases are that an unauthorized user will gain access to the VG Marketing Plans, on Sally's workstation, by utilizing Mark's insecure computer. Since the high value asset is located in a highly secure room, the intranet connection is the most likely vulnerability the classified asset faces. In each of the scenarios, for this test case, only the intranet connection was altered from scenario

to scenario. Physical security for the entire *VentureGames'* office building, and for the highly secured walled office, remained constant throughout each test scenario.

The following table delineates each test scenario with the test designer's expected pre-test execution results.

Test ID	Test Parameters	Expected Results
VGTest2a.	Sally's workstation is not connected to the Intranet.	Sally will be able to access the marketing plans and they will not be disclosed.
VGTest2b.	Sally's workstation is connected to the intranet via a router. There is no protection against the network.	Sally will be able to access the marketing plans however the lack of protection from the network will result in their unauthorized disclosure.
VGTest2c.	Sally's workstation is connected to the intranet via a firewall. The firewall is configured to block all traffic in both directions. This should be similar to having no connection to the intranet.	Sally will be able to access the marketing plans and the firewall will protect the asset from unauthorized disclosure.
VGTest2d.	Sally's workstation is connected to the intranet via a firewall. The firewall is configured to block all traffic in to her workstation while allowing her access to the employee files out on the intranet.	Sally will be able to access the marketing plans and the firewall will protect the asset from unauthorized disclosure.

Table 4. VGTest2 Expected Results

c. Actual Results

The test scenarios for Test Case 2 were conducted in the same fashion as those in Test Case 1, i.e. observed during execution and results files inspected after test completion. Additionally, for testing consistency, all test cases were conducted using the same CyberCIEGE game engine. The results of the test scenarios varied from scenario to scenario, therefore, the following table provides a summary of the actual results experienced and identifies whether they met the designers expectations:

Test ID	Actual Results	Met Expectations
VGTest2a.	Sally was able to access her office and workstation. She had access to the marketing plans, and the plans were not compromised.	Yes
VGTest2b.	Sally was able to access her office and workstation. She had access to the marketing plans, but the plans were compromised through the unprotected network connection	Yes
VGTest2c.	Sally was able to access her office and workstation. She had access to the marketing plans, but the plans were compromised even though they were being protected by a firewall with filters set to block all traffic in and out.	No
VGTest2d.	Sally was able to access her office and workstation. She had access to the VG Marketing Plans on her workstation and access to the employee files on the intranet. However, the marketing plans were compromised even though they were being protected by a firewall with filters set to block all traffic coming in to Sally's system.	No

Table 5. VGTest2 Actual Results

In this set of tests, both test scenarios VGTest2a and VGTest2b met expectations. In test scenario VGTest2a, Sally's workstation had no network connection and was located in a highly protected office (physical security set to 900+). Thus it should have remained secure, with an attacker motivation of 300, and it did. In test scenario VGTest2b, Sally's workstation was connected to the network, but no network protection was provided. Therefore, the marketing plans should have been disclosed, and they were.

Test scenarios VGTest2c and VGTest2d were designed to test the game engines ability to model the functionality that a firewall provides. In test scenario VGTest2c, a firewall was used to logically separate Sally's workstation from the rest of the network. The firewall filters were set to block all network traffic into and out of Sally's personal intranet. The results of this test scenario should have been similar to those of test scenario VGTest2a, in which there was no connection to the network. Sally's workstation, and the classified asset, should have been secure, however the CyberCIEGE game engine did not properly model the functionality provided by a firewall and its filters. The classified asset was not protected and Sally's workstation was not logically isolated from the rest of the network.

In test scenario VGTest2d, the firewalls were utilized to logically isolate Sally's workstation from the rest of the network while still enabling her to gain access to an asset through the intranet. This test scenario, like the previous one, was designed to validate whether the game engine properly modeled the functionality of firewalls and their filters. The firewall filters were set to allow Sally access out to the intranet while simultaneously blocking access into her system and from it. While Sally was able to gain access to the intranet, the firewall failed to protect the classified asset located on her protected system.

Test Case 2 successfully identified an area of concern with the CyberCIEGE game engine. The results of these test scenarios, failure of the CyberCIEGE game engine to properly model the functionality provided by firewalls and filters, have been forwarded to the game engine developers for correction. As of the date of the writing of this thesis, this issue has not yet been corrected.

3. Test Case 3 "Internet"

a. Test Goal and Design

Connection to an external network (Internet) introduces numerous new vulnerabilities that have to be addressed in order to ensure confidentiality. In Test case 3 the need for just such a connection is introduced. The goal of this test case is to identify the basic secrecy issues involved with connecting to an external network and to identify some basic measures that can be taken to provide security for confidential information

For testing purposes, all of the "Internet" test scenarios will have a high level of physical security. This will focus the test case on the Internet connection as being the potential vulnerability for the confidentiality requirement. Security measure on the workstation, such as virus protection and patches, will not be implemented in order to focus the test on the security provided by the network security measures put in place.

Sally is in charge of marketing at *VentureGames*. She is a trusted user and possesses a security clearance. Sally's goal is to access the VG Marketing Data (asset) on her workstation. Her workstation is connected to the Internet. The Marketing Data on Sally's workstation is confidential information and needs protection. Sally is the only

user authorized to enter her office (zone) and to access her workstation. The overall goal of this test case is to identify game configurations that protect the classified information on Sally's workstation from unauthorized access and to determine whether the CyberCIEGE game engine properly models the scenarios.

To conduct this test case, six smaller test scenarios were developed. These smaller test scenarios each focused on different game configurations and aspects of Internet connection. The configurations in the test scenarios are: No Internet connection, Internet connection through a router, Internet connection through a firewall with no filters, Internet connection through a firewall that blocks all traffic in and out, Internet connection through a firewall that blocks all traffic in and out except telnet, and an Internet connection through a firewall that blocks all traffic in and out except email and web browsing. These smaller scenarios are needed to identify the effects of different network configurations on the protection of the classified asset. The titles of each of these test scenarios are:

- VGTest3a_Conf_Internet_Routers_No-Access.sdf
- VGTest3b_Conf_Internet_Routers_Access.sdf
- VGTest3c_Conf_Internet_Firewall_No-Filters.sdf
- VGTest3d_Conf_Internet_Firewall_Filters_Block-All-BothDir.sdf
- VGTest3e_Conf_Internet_Firewall_Filters_Telnet.sdf
- VGTest3f_Conf_Internet_Firewall_Filters_Web-Email.sdf

b. Expected Results

In this set of test scenarios Sally should have access to her office, her workstation, and the VG Marketing Data. Each test scenario will then change the network configuration only, to validate that the game engine properly identifies and models the vulnerabilities associated with connecting to the Internet. Additionally, these test scenarios will identify security measures that the player can take to mitigate these vulnerabilities. There are six test scenarios in this test case. Each of the Test Case 3 scenarios was executed several times. In each execution all parameters remained constant, except the attacker motivation. Attacker motivation was changed (00, 25, 50,

100, 400, 800) in each scenario to determine if the game engine recognized the difference in attacker motivation and properly escalated the attack.

In general, when the scenarios had lower attack motivations the vulnerabilities associated with the Internet connection should be less accessible than when the attacker motivation was elevated. For example, in the test scenario with no Internet connection, VGTest3a, the classified asset should be protected from unauthorized disclosure, regardless of the attacker motivation, since the physical protection afforded (835) is greater than the maximum attacker motivation (800) tested. While in scenario VGTest3b, where the workstation is connected to the Internet through a router, there should be numerous vulnerabilities that the game engine should identify. The game engine should also utilize these vulnerabilities to gain access to the classified information. In this test scenario the asset should be disclosed rather easily. Changing the connection to the Internet from a router to a firewall, in VGTest3c, should provide some protection for the asset. At very low attacker motives the asset should be protected but as the attacker motive increases the asset should be easily accessed and disclosed. Adding filters to the firewall, in VGTest3d, that block all network traffic in and out should provide sufficient protection to the asset so that it is not disclosed at any attacker motivation in the test. This scenario should have results that are similar to the no Internet connection scenario, VGTest3a. In the fifth test scenario, VGTest3e, all traffic except for Telnet is blocked in both directions. Permitting the use of Telnet provides the attacker with a vulnerability that can be used to access the classified information. The asset should eventually be disclosed through this vulnerability. The final test scenario, VGTest3f, models a common configuration in the corporate world. The firewall is configured to block all traffic except for web browsers and email from coming in or out of the network. Web browsing and email communications are often paramount to the productive and happy performance of a company's employees, however they do provide a vulnerability that an attacker can use to gain access to the classified information. For this test scenario, the game engine should identify this vulnerability and utilize it to disclose the classified information.

The following table provides a summary of the test parameters for each scenario and the test designer's expected results:

Test ID	Test Parameters	Expected Results
VGTest3a.	Sally's workstation and the classified asset are located in a highly secure (835) room and are not connected to the Internet.	Sally will have access to her office, workstation and the asset. The asset will not be disclosed regardless of attacker motive.
VGTest3b.	Sally's workstation and the classified asset are located in a highly secure (835) room. Her workstation is connected to the Internet via a router. There is no network protection in place.	Sally will have access to her office, workstation and the asset. The asset will be disclosed through the unprotected Internet connection as the attacker motivation increases.
VGTest3c.	Sally's workstation and the classified asset are located in a highly secure (835) room. Her workstation is connected to the Internet via a firewall. There are no filters set.	Sally will have access to her office, workstation and the asset. The asset will be disclosed through the unprotected Internet connection as the attacker motivation increases.
VGTest3d.	Sally's workstation and the classified asset are located in a highly secure (835) room. Her workstation is connected to the Internet via a firewall. The firewall filters are set to block all network traffic coming in and going out.	Sally will have access to her office, workstation and the asset. The asset will not be disclosed regardless of attacker motive. The firewall should logically separate Sally's workstation from the Internet so that no unauthorized access is gained.
VGTest3e.	Sally's workstation and the classified asset are located in a highly secure (835) room. Her workstation is connected to the Internet via a firewall. The firewall filters are set to block all network traffic coming in and going out, except for Telnet.	Sally will have access to her office, workstation and the asset. The asset should eventually be disclosed as the attacker motive increases. Since the Telnet access provides a vulnerability that a highly motivated attacker should be able to use to gain unauthorized access.
VGTest3f.	Sally's workstation and the classified asset are located in a highly secure (835) room. Her workstation is connected to the Internet via a firewall. The firewall filters are set to block all network traffic coming in and going out, except for e-mail and web browsers.	Sally will have access to her office, workstation and the asset. The asset should eventually be disclosed as the attacker motive increases. Since the e-mail and web browser access provide vulnerabilities that a highly motivated attacker should be able to use to gain unauthorized access.

Table 6. VGTest3 Expected Results

c. Actual Results

The test scenarios, for Test Case 3, were conducted in the same fashion as the previous two test cases, i.e. the game simulation was observed during execution and results and log files were inspected after test completion. All test parameters remained constant in each test scenario except for the degree of attacker motivation. The attacker's motive, for gaining unauthorized access to the confidential asset, varied (0, 25, 50, 100, 200, 800), in each execution of the test scenario. This was done in order to test both the degree of security provided by each network component and the game engine's ability to recognize vulnerabilities and properly model attacks based on them.

The following table provides a summary of the actual results experienced and identifies whether they met the test designer's expectations:

Test ID	Actual Results	Met Expectations
VGTest3a.	Sally was able to access her office, workstation, and the marketing plans. The plans were not compromised at any level of attacker motivation.	Yes
VGTest3b.	Sally was able to access her office, workstation, and the marketing plans. The plans were compromised; however, the compromise did not occur until the attacker motivation reached 25.	Yes
VGTest3c.	Sally was able to access her office, workstation, and the marketing plans. The plans were compromised; however, the compromise did not occur until the attacker motivation reached 25. (It would have been preferable if the firewall had been slightly more secure than a router but this was not a requirement for this test.)	Yes
VGTest3d.	Sally was able to access her office, workstation, and the marketing plans. The plans were not compromised and were protected by the firewall with filters set to block all network traffic in and out. The results were similar to VGTest3a, no internet connection.	Yes
VGTest3fe.	Sally was able to access her office, workstation, and the marketing plans. The plans were compromised, however, the compromise did not occur until an attacker value of 200.	Yes
VGTest3f.	Sally was able to access her office and workstation. She had access to the VG Marketing Plans. The plans were compromised. The compromise occurred at an attacker	No

	value of 25. This put the attack in the range of amateur hackers and script kiddies.	

Table 7. VGTest3 Actual Results

The results of Test Case 3 met, for the most part, the expectations of the test designer. Unprotected Internet access resulted in the compromise of classified assets, at even low attacker motives, while providing network security components, i.e. firewalls, provided some protection from unauthorized access via the Internet. Additionally the game engine properly simulated the types of attacks (i.e. Trojan horse and Hacker attacks) and increased both the number and success of the attacks as the attacker motive was escalated.

One discrepancy identified during this test was the performance of the firewalls and filters. In Test Case 2, utilizing a firewall to isolate and protect a classified system from an Intranet, the firewalls and filters provided no security to the classified asset. However, in Test Case 3, utilizing a firewall to protect classified system from the Internet, the firewall and filters performed as the test designer expected. This discrepancy, in the performance of firewalls, was identified and forwarded to the CyberCIEGE game engine developers and will be corrected on a later version of the game.

C. SUMMARY

The test cases developed for this thesis were designed to test some basic aspects concerning the confidentiality of classified information and to validate whether the CyberCIEGE game engine properly modeled and simulated these aspects. Overall the tests conducted were successful. Numerous test scenarios were developed to test the game engine. These test scenarios were designed to challenge the game engine in a different way and to isolate and identify its ability to properly model and simulate, in a realistic manner, the virtual environment developed by the test designer.

Several areas of concern with the game engine were identified through these tests. Some of these concerns were minor, and were immediately corrected. Some concerns

were corrected in subsequent revisions of the game engine, while other concerns, about the game engine's performance, have yet to be addressed. Follow-on testing, and improvements to the game engine are still necessary, but the results of these tests show that the game engine functions, with some exceptions, in an acceptable manner.

VI. RECOMMENDATIONS & CONCLUSION

A. RECOMMENDATIONS

1. CyberCIEGE Game Play Issues

The conduct of this thesis coincided with the development of the CyberCIEGE game engine. Numerous versions of the game engine were utilized during this thesis. As issues concerning the game engine's performance arose they were immediately identified and forwarded to the game engine developers. However, not all of the issues identified have been addressed or corrected by the completion date of this thesis. Therefore, there remain some game play issues in the current version of the game. Some of these game play issues are major concerns that affect the overall function of the game (i.e. firewalls) and have been addressed, both in this thesis and by other means, while others are not as critical, but do affect the training and entertainment value, as well as the game's playability.

The following sections identify some recommended improvements to the CyberCIEGE game. These improvements, if incorporated into the game engine prior to its official release, will improve the overall playability of the game and thus its successful launch as an Information Assurance Virtual Laboratory.

a. Firewalls

Firewalls represent an essential tool, in both civilian and military, network defense. They are one of the most common, and effective, means for isolating internal networks and protecting classified information. The firewall component in the CyberCIEGE game does not currently function in a realistic manner. There were several areas in which the firewalls need to be corrected in the simulation engine.

First the firewalls need to be corrected in their basic functionality. The firewall, and associated filters, in the Internet test cases functioned in a reasonable manner, only needing some minor fine-tuning, while the firewall and filters in the Intranet test case did not function at all[5]. The firewalls, in the CyberCIEGE game,

[5] The same version of the game engine was used to test both the firewalls in the Internet test cases and the Intranet test cases.

represent a critical component in the defense of a network. The basic functionality of the firewalls, within the game, must be addressed and corrected so that they properly simulate the functionality and performance of firewalls in the real world. This is essential for the game to achive its educational objectives.

The second area, which needs to be addressed, is the filtering of traffic into and out of the firewall. Currently the direction of network traffic is modeled in relation to the network, not the firewall port in which the traffic is entering or leaving. This does not represent, in a realistic manner, the way an actual firewall is configured. The difference between the way a CyberCIEGE firewall is configured and how one in the real world is configured causes both confusion for the player, when attempting to utilize a firewall in the game, and does not properly educate the player in the basic concepts associated with configuring a real firewall.

The following diagrams provide an example of the differences in the configuration aspects of a CyberCIEGE firewall and a real firewall. As will be demonstrated in the examples, there is a difference in perspective when setting the firewall's filters which can be counterintuitive to the player. In a real world firewall, the filters are set with the perspective of the firewall taken into account. This means that if a filter is set to block traffic in, the filter will block traffic coming into the firewall from the connected network. In the CyberCIEGE game, the perspective of the network is taken. In these CyberCIEGE firewalls, if a filter is set to block traffic in, the filter will block traffic flowing from the firewall and into the network. While these differences are easily overcome, once the perspective is explained to the player, they add an unnecessary degree of confusion to the game and do not fulfill the requirements to educate the player in the basic functionality of a firewall.

In each diagram the firewall filters are set to block all traffic in for Network 1 and block all traffic out for Network 2. These examples illustrate the differences in the flow of traffic in the two configurations.

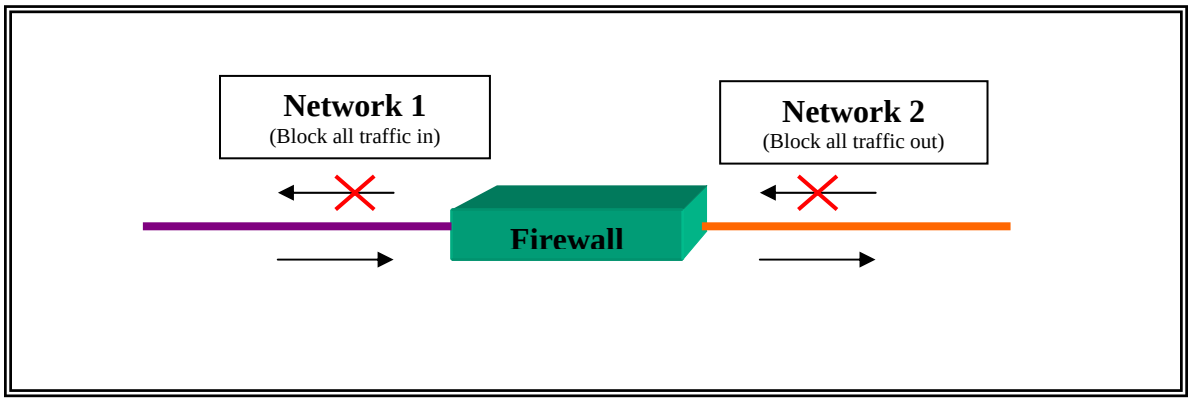

Figure 1. CyberCIEGE firewall filter performance

Figure 1 illustrates the functionality experienced in a CyberCIEGE firewall. In this example the firewall's filters are set in the following manner: Network 1 – Block All Traffic In; Network 2 – Block All Traffic Out. As demonstrated in this example, this results in all traffic flowing **into** Network 1 from the firerwall to be blocked and all traffic flowing **out of** Network 2 and into the firewall to be blocked. The next figure will demonstrate the way a real world firewall functions.

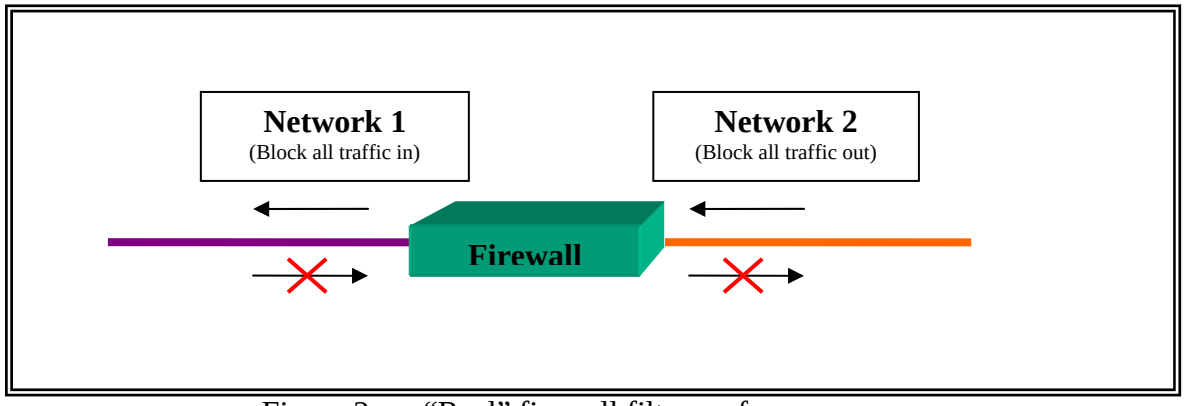

Figure 2. "Real" firewall filter performance

Figure 2 illustrates the functionality experineced in a real world firewall. In this example the firewall's filters are set in the same manner as in the first example: Network 1 – Block All Traffic In; Network 2 – Block All Traffic Out. As demonstrated in this example, this results in all traffic flowing **into the firewall** from Network 1 to be blocked and all traffic flowing **out of the firewall** into Network 2 to be blocked.

These differences, between the firewalls' functionality, are counterintuitive and can cause confusion for the player while plaing the game. The CyberCIEGE firewalls should be adjusted so that they more accurately reflect real world firewall functionality. These differences are a concern because they pose a major hindrance to the training and education aspects of the game as well as to its playability. For the CyberCIEGE project to fulfill its educational goals, the functionality of the firewalls within the game must be corrected.

b. Virtual Users

Each virtual user in the CyberCIEGE game has many personalization parameters. These parameters establish such things as the user's sex, description, and asset goals. They also establish the user's initial happiness and productivity levels. During the execution of the game, these happiness and productivity levels can be affected by events within the game. These events include the establishment of physical security measures, i.e. installing cipher locks or hiring a guard, or the user's inability or difficulty in accomplishing his goal, i.e. having to use two separate workstations or having to go from one zone to another to accomplish this goal.

While the virtual user sensitivity is an important aspect for both the game's playability and player's educational benefit, the current level of sensitivity needs to be better tuned to provide a more realistic simulation of a virtual user's reaction to such events. Additionally, a trigger or parameter should be established that allows the scenario designer the discretion to either turn off or on a virtual user's sensitivity or to be able to better adjust it so that differences in virtual user's personalities and backgrounds can be simulated. For example, a military virtual user is going to be less sensitive to strict physical security measures than perhaps a civilian virtual user, while the leader of an organization may be more sensitive to productivity issues than an entry-level employee. Fixing the CyberCIEGE game engine so that these differences in virtual user sensitivities can be simulated will enhance both the game's playability and the user's educational benefit derived from the game.

c. Malicious Software Occurrence

The CyberCIEGE game engine simulates the occurrence of various types of malicious software. This malicious software includes such things as computer viruses[6] and Trojan Horses[7]. These types of malicious software represent a significant threat to the protection of information. They are abundant and new versions of them are constantly being developed and released to undermine any preventative security measures established to counter them. In the CyberCIEGE game, however, the persistent infection of these types of malicious software can be detrimental to the educational goal of the scenario designer. Since the CyberCIEGE game was developed to educate players on numerous aspects and levels of information assurance and network security the scenario designer needs to have the ability to determine the amount and type of potential malicious software that occurs in a given scenario. The current game configuration automatically introduces malicious software on low assurance components and provides constant *ticker*[8] messages informing the player of the presence of this software.

Currently there is no way for a scenario designer to control the introduction of malicious software on components in the game. Additionally, there is no way for the scenario designer to control, i.e. eliminate, the constant *ticker* message traffic scrolling across the screen. The persistent occurrence of this malicious software on components and the constant barrage of *ticker* message traffic can detract from the intended educational goal of the scenario designer. For example, in the physical security tests conducted for this thesis, a new player to the game may lose sight of his intended scenario goal, i.e. physically securing a classified asset, due to the constant barrage of messages identifying malicious software that has been installed on a workstation. This software has no effect on the security of the classified asset, since the workstation is not connected to a network, however the player may feel the need to address this issue, thus distracting him from the intended educational goal of the scenario designer. Therefore, the scenario designer

---

[6] Webopedia defines a computer virus as: "A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes."

[7] Webopedia defines a Trojan Horse as: "A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive."

[8] A ticker message is a message to the player that scrolls across the bottom of the game screen.

needs a mechanism to either control or eliminate the malicious software, and associated message traffic, for a scenario.

2. Future Work

This thesis focused on determining whether a CyberCIEGE scenario could be developed that was both educational and a playable game. Through the use of test cases and the development of the *VentureGames'* CyberCIEGE scenario this thesis has demonstrated that a playable CyberCIEGE game can be designed using Scenario Definition Files (SDF). However, some modifications to the SDFs and game engine tuning are still required. Additionally, this thesis demonstrated the possibility of designing CyberCIEGE scenarios that provide an educational benefit to the player. This thesis developed a CyberCIEGE game that, when played, introduces information assurance and network security issues to the player in an incremental, educational, and entertaining manner. However, this thesis did not provide a metric to validate or quantify the degree of educational benefit the player derived from the game.

The logical next step in the development of the CyberCIEGE game is to develop a metric that can be used to provide quantifiable data that validates the educational benefit of the game. To do this, players with an identifiable degree of pre-existing information assurance and network security knowledge, preferably none, must be utilized. The players could be given a pre-game play questionnaire, designed to identify their pre-existing understanding of information assurance and network security, and then a post-game play questionnaire, designed to identify their post CyberCIEGE understanding of information assurance and network security. Numerous test players will be required in order to obtain statistically significant data. Once the basic premise that the game provides an educational benefit to the player is proven, more advanced tests must be conducted to identify the ability of the CyberCIEGE game to provide an educational benefit to a range of players with varying degrees of pre-existing information assurance and network security knowledge.

B. CONCLUSION

This thesis contributes to the ongoing research involved with the CyberCIEGE project that is being conducted at the Naval Postgraduate School in Monterey California. As stated earlier, the mission of the project is to "create an Information Assurance (IA) teaching/learning laboratory."[Irvine 2003] This thesis fulfills an essential step required for the project to reach its stated goals.

This thesis answered two fundamental questions concerning the CyberCIEGE project. The first question answered is: can a CyberCIEGE scenario be developed such that it is simultaneously a playable game and an educational tool that illustrates confidentiality issues in an internal corporate network connected to the Internet? Clearly the answer to this question is yes. The *VentureGames'* scenario is a fully playable, five module, CyberCIEGE game that can both be won or lost, based on decisions the player makes. The game provides ample feedback to the player in the form of ticker and pop-up[9] messages as well is in the increase and decrease of the player's available money. Additionally, by incrementally increasing the complexity of the modules and expounding on the lessons learned from each previous one the *VentureGames'* scenario provides an educational benefit to the player, the degree of educational benefit must be quantified in follow-on work.

The second question answered by this thesis was: is it possible to validate that the CyberCIEGE game engine produces expected results from a predefined scenario definition file? This thesis clearly demonstrates that the answer to this question is yes, as well. Numerous discrepancies, failings, and performance errors in the game engine were identified during the testing and game development phases of this thesis. The large number of these events is attributable to the fact that the CyberCIEGE game engine was still underdevelopment during the conduct of this thesis. The game engine developers were quickly notified of these discrepancies. Many of them were fixed immediately, while others are scheduled to be corrected in later versions of the game. This clearly shows that a scenario designer can validate the game engine's ability to produce results, that met the designer's expectations, from a predefined scenario definition file.

[9] A pop-up message is a message to the player that is displayed in a dialogue window that appears on the game screen. The player must acknowledge the message before resuming the game.

Training and educating Information Technology (IT) users in the arena of information assurance and network security is a very complex and daunting task. These users often have varying degrees of pre-existing knowledge, educational level, trustworthiness, and security clearances that the IT professional must take into account when developing a training program. Additionally, the IT users are often not interested in or too busy to attend essential, and often required, IT training. If users do attend training, the educational benefit derived from it is often far below what is required. Factor in the increasing reliance on technology to perform mission critical functions as well as the increased utilization of networks as a means for accessing, transmitting, and storing information and today's IT professional is facing an exponentially increasing problem when it comes to providing essential It training to his users.

The CyberCIEGE project provides one possible solution to this problem through the use of customizable scenarios that can be tailored, by the scenario designer, to meet the specific IT training needs of individual users. Furthermore, the CyberCIEGE game provides this training in the form of an entertaining, commercial grade, computer game that educates while it entertains. Additionally, since the CyberCIEGE game can be loaded onto any modern personal computer, or laptop computer, users can fulfill their training requirements from virtually anywhere, i.e. from their desk, on travel, or at home. This aspect of the CyberCIEGE game reduces the need to organize and schedule large, time consuming, mass training sessions that waste both the user and organization's time and do not fully meet the training needs of either. CyberCIEGE represents a revolutionary new tool that IT professionals can employ to better meet the security needs of their users and their organizations.

APPENDIX A – TEST CASES

This Appendix contains the test case SDFs that were developed for, and described in, this thesis.

The Appendix is accessible via following link:

http://library.nps.navy.mil/uhtbin/hyperion/04Sep_Lamorie_Appendices.doc

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – VENTUREGAMES' SCENARIO

This Appendix contains the *VentureGames'* SDFs that were developed for, and described in, this thesis.

The Appendix is accessible via following link:

http://library.nps.navy.mil/uhtbin/hyperion/04Sep_Lamorie_Appendices.doc

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C – VENTUREGAMES' SCENARIO SOLUTIONS

This Appendix contains the possible solutions to the *VentureGames'* SDFs that were developed for, and described in, this thesis.

The Appendix is accessible via following link:

http://library.nps.navy.mil/uhtbin/hyperion/04Sep_Lamorie_Appendices.doc

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D – VENTUREGAMES' WORKSPACE FILE

This appendix contains the workspace files for the VentureGames CyberCIEGE scenario. A workspace files determines the position of the user workspaces and which workspaces are active and which are not. The workspace file contains a list of data, which determine the direction, location, and activity (A = Active, I = inactive) of a workspace. This data comes in the following form: Direction, Latitude, longitude, activity (i.e. N 53 96 A). The first letter (N, S, E, or W,) indicates in what direction the workspace faces. The location of the workspace is determined by a two number coordinate (latitude and longitude) of the desired workspace location within the game. Finally, the last letter (A or I) indicates whether the workspace is active or inactive. Workspaces files can be customized for each scenario to improve game play and increase the entertainment value of the game. Two workspace files were used during this thesis.

The Appendix is accessible via following link:

http://library.nps.navy.mil/uhtbin/hyperion/04Sep_Lamorie_Appendices.doc

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[Albion 2004] *Computer Security: A Practical Definition* (n.d.). Retrieved (April 2004) from the World Wide Web: http://www.albion.com/security/intro-4.html

[ClickZ 2004] ClickZ stats staff. (2004). *Population Explosion*! Retrieved (July 2004) from the World Wide Web: http://www.clickz.com/stats/big_picture/geographics/article.php/5911_151151

[CNN 2003] CNN.com (2003). Belgium's 'Biggest Diamond Heist'. Retrieved (July 2004) from the World Wide Web: http://www.cnn.com/2003/WORLD/europe/02/18/belgium.diamonds.ap/**[CNSS 2003]** CNSS Instruction 4009, (Revised 2003). *National Information Assurance (IA) Glossary*. Retrieved (April 2004) from the World Wide Web: http://www.nstissc.gov/Assets/pdf/4009.pdf

[Hoffman 2004] Hoffman, D., Novak, T., Venkatesh, A. (July 2004). *Has the Internet Become Indespensible?*. Communications of the ACM. Retrieved (August 2004) from the World Wide Web: http://portal.acm.org/citation.cfm?id=1005818

[Cyber 2003] *CyberCIEGE (Corporate Information Educational Gaming Environment).* (n.d.). Retrieved (December 2003) from the Naval Postgraduate School Intranet: http://cisr.nps.navy.mil/projectsimsec.html

[DIOR 2004] Directorate for Information Operations and Reports – Statistical Information Analysis Division. Retrieved (April 2004) from the World Wide Web: http://web1.whs.osd.mil/mmid/mmidhome.htm

[DoN 1999] Department of the Navy (DoN) Information Security Program (ISP) Regulation, SECNAV Instruction 5510.36 Chapter 4, Classification Management; Retrieved (April 2004) from the World Wide Web: http://neds.nebt.daps.mil/551036.htm

[Fisher 2003] Fisher, C., Chiricosta, T. & Witherspoon, T. (2003). *Software Testing Workshop*. Proceedings of the STC 45th Annual Conference, Anaheim, California. Retrieved (February 2003) from the World Wide Web: http://www.ocstc.org/ana_conf/pdf/tt7s.pdf

[ITSecurity 2004] ITSecurity.com (2004). *Dictionary of Information Security*. Retrieved (July 2004) from the World Wide Web: http://www.itsecurity.com/dictionary/dictionary.htm

[Irvine 2002] Irvine, C. & Thompson, M. (2002). *SimSecurity -- Can You Keep the Network Alive?* Naval Postgraduate School Center for Information Systems Security Studies and Research. Retrieved (September 2003) from the World Wide Web: http://cisr.nps.navy.mil/SimSecurity/web/SimSecurity.html

[Irvine1 2003] Irvine, C. & Thompson, M. (2003, June). *Teaching Objectives of a Simulation Game for Computer Security*. Proceedings of Informing Science and Information Technology Joint Conference, Pori, Finland.

[Irvine2 2003] Irvine, C. (2003, May). *The SimSecurity Information Assurance Virtual Laboratory*. Proceedings of IEEE Security & Privacy conference, Oakland, California.

[Johns 2004] Johns, Ken. (2004). *Toward Managing & Automating CyberCIEGE Scenario Definition File Creation.* Master of Science Thesis, Department of Computer Science, Naval Postgraduate School.

[Pressman 2001] Pressman, R. (2001). *Software Engineering: A Practitioner's Approach 5th ed.* Boston: Mc Graw Hill.

[Rivermind1 2002] Rivermind, Inc. & Naval Postgraduate School Center for Information Systems Security Studies and Research (2002). *CyberCIEGE: Scenario Format Template*.

[Rivermind2 2002] Rivermind, Inc. & Naval Postgraduate School Center for Information Systems Security Studies and Research (2002). *CyberCIEGE: Encyclopedia.*

[Saltzer 1975] Jerome, S. & Schroeder, M. (1975, September). *The Protection of Information in Computer System*. Proceedings of the IEEE, vol. 63, no. 9, pp. 1278-1308.

[Southgate 2002] Southgate, D. (2002). *Lack of Training Your Biggest Threat.* TechRepublic Retrieved (July 200w) from the World Wide Web: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2894933-1,00.html

[Teo 2002] Tiat Lang, T. (2002). *Scenario Selection and Student Assessment Modules for CyberCIEGE*. Master of Science Thesis, Department of Computer Science, Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Marine Corps Representative
   Naval Post Graduate School
   Monterey, CA

4. Director, Training and Education
   MCCDC, Code C46
   Quantico, VA

5. Director, Marine Corps Research Center
   MCCDC, Code C40RC
   Quantico, VA

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, CA

7. George Bieber
   OSD
   Washington, DC

8. RADM Joseph Burns
   Fort George Meade, MD

9. Bill Chinn
   Rivermind
   Mountain View, CA

10. Deborah Cooper
    DC Associates, LLC
    Roslyn, VA

11. CDR Daniel L. Currie
    PMW 161
    San Diego, CA

12. Louise Davidson
National Geospatial Agency
Reston, VA

13. LCDR James Downey
NAVSEA
Washington, DC

14. Diane Gant
National Science Foundation
Arlington, VA

15. Richard Hale
DISA
Falls Church, VA

16. LCDR Scott D. Heller
SPAWAR
San Diego, CA

17. Wiley Jones
OSD
Washington, DC

18. Russell Jones
N641
Arlington, VA

19. Hun Kim
Department of Homeland Security
Washington, DC

20. David Ladd
Microsoft Corporation
Redmond, WA

21. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

22. Steve LaFountain
NSA
Fort Meade, MD

23. Larry Frank
    Department of Homeland Security
    Washington, DC

24. Dr. Greg Larson
    IDA
    Alexandria, VA

25. Penny Lehtola
    NSA
    Fort Meade, MD

26. Ernest Lucier
    Federal Aviation Administration
    Washington, DC

27. Dr. Vic Maconachy
    NSA
    Fort Meade, MD

28. Doug Maughan
    Department of Homeland Security
    Washington, DC

29. CAPT Sheila McCoy
    Headquarters U.S. Navy
    Arlington, VA

30. John Mildner
    SPAWAR
    Charleston, SC

31. Dr. John Monastra
    Aerospace Corporation
    Chantilly, VA

32. Brian Morgan
    Rivermind
    Mountain View, CA

33. Dr. Roger Schell
    Aesec
    Pacific Grove, CA

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

35. Dr. Ralph Wachter
ONR
Arlington, VA

36. David Wirth
N641
Arlington, VA

37. Daniel Wolf
NSA
Fort Meade, MD

38. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

39. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

40. Michael F. Thompson
Naval Postgraduate School
Monterey, CA

41. Paul C. Clark
Naval Postgraduate School
Monterey, CA

42. Justin Lamorie
Student, Naval Postgraduate School
Monterey, CA