2011-12

A cyberciege traffic analysis extension for teaching network security

Chang, Xuquan Stanley.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/10578

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBERCIEGE TRAFFIC ANALYSIS EXTENSION FOR TEACHING NETWORK SECURITY

by

Xuquan Stanley Chang
Kim Yong Chua

December 2011

Thesis Co-Advisors:	Robert Beverly John D. Fulp Michael Thompson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE A CyberCIEGE Traffic Analysis Extension for Teaching Network Security	**5. FUNDING NUMBERS**
6. AUTHOR(S) Chang Xuquan Stanley and Chua Kim Yong	
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. IRB Protocol number ______N/A__________.

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

13. ABSTRACT (maximum 200 words)

CyberCIEGE is an interactive game simulating realistic scenarios that teaches the players Information Assurance (IA) concepts. The existing game scenarios only provide a high-level abstraction of the networked environment, e.g., nodes do not have Internet protocol (IP) addresses or belong to proper subnets, and there is no packet-level network simulation. This research explored endowing the game with network level traffic analysis, and implementing a game scenario to take advantage of this new capability. Traffic analysis is presented to players in a format similar to existing tools such that learned skills may be easily transferred to future real-world situations.

A network traffic analysis tool simulation within CyberCIEGE was developed and this new tool provides the player with traffic analysis capability. Using existing taxonomies of cyber-attacks, the research identified a subset of network-based attacks most amenable to modeling and representation within CyberCIEGE. From the attacks identified, a complementary CyberCIEGE scenario was developed to provide the player with new educational opportunities for network analysis and threat identification. From the attack scenario, players also learn about the effects of these cyber-attacks and glean a more informed understanding of appropriate mitigation measures.

14. SUBJECT TERMS **Information Assurance, Network Security, Computer Security, Traffic Analysis, CyberCIEGE, Training**	**15. NUMBER OF PAGES** 115
	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** UU

THIS PAGE INTENTIONALLY LEFT BLANK

A CYBERCIEGE TRAFFIC ANALYSIS EXTENSION FOR TEACHING NETWORK SECURITY

Xuquan Stanley Chang
Civilian, Defence Science & Technology Agency, Singapore
B.Eng., National University of Singapore, 2006

Kim Yong Chua
Civilian, Defence Science & Technology Agency, Singapore
B.Eng., Nanyang Technological University, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Xuquan Stanley Chang

Kim Yong Chua

Approved by: Robert Beverly
Thesis Co-Advisor

John D. Fulp
Thesis Co-Advisor

Michael F. Thompson
Thesis Co-Advisor

Peter J. Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

CyberCIEGE is an interactive game simulating realistic scenarios that teaches the players Information Assurance (IA) concepts. The existing game scenarios only provide a high-level abstraction of the networked environment, e.g., nodes do not have Internet protocol (IP) addresses or belong to proper subnets, and there is no packet-level network simulation. This research explored endowing the game with network level traffic analysis, and implementing a game scenario to take advantage of this new capability. Traffic analysis is presented to players in a format similar to existing tools such that learned skills may be easily transferred to future real-world situations.

A network traffic analysis tool simulation within CyberCIEGE was developed and this new tool provides the player with traffic analysis capability. Using existing taxonomies of cyber-attacks, the research identified a subset of network-based attacks most amenable to modeling and representation within CyberCIEGE. From the attacks identified, a complementary CyberCIEGE scenario was developed to provide the player with new educational opportunities for network analysis and threat identification. From the attack scenario, players also learn about the effects of these cyber-attacks and glean a more informed understanding of appropriate mitigation measures.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

API	Application Programming Interface
ARP	Address Resolution Protocol
AVOIDIT	Attack Vector, Operational Impact, Defense, Information Impact, and Target
CAS	Cyber Attack Simulator
CERT	Computer Emergency Response Team
CISR	Center for Information Systems Security Studies and Research
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DISA	Defense Information Systems Agency
DNS	Domain Name Server
DOM	Document Object Model
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IDS	Intrusion Detection Systems
IP	Internet Protocol
ISWGS	Information Security War Gaming System
IT	Information Technology
LAN	Local Area Network
MAADNET	Military Academy Attack/Defense Network
MAC	Media Access Control
MMORPG	Massively Multiplayer Online Role-playing Game
MO	Method of Operation
MTA	Mail Transfer Agent
OTP	One-Time Password
PCAP	Packet Capture
PDML	Packet Details Markup Language
PGA	Professional Gamers Association

PSML	Packet Summary Markup Language
RFC	Request for Comment
SAX	Simple API for XML
SDF	Scenario Definition File
SDT	Scenario Development Tool
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our gratitude to Dr. Robert Beverly, John D. Fulp and Michael Thompson for their inspiring and valuable guidance during the course of this thesis. Thank you for your patience and constructive feedback.

We would also like to thank our families for their understanding and support. It has been a difficult time for them during the period of separation when they were in Singapore while we were doing our studies in the United States.

We also wish to thank our sponsor, Defence Science and Technology Agency (DSTA) of Singapore, for granting us the opportunity to be part of this enriching joint program between the National University of Singapore and the Naval Postgraduate School. The one-year stay in Monterey has been a wonderful experience.

Finally, we would also like to thank Janet Werner for her excellent and professional support in editing our thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS STATEMENT

This thesis research is part of an extension to the ongoing project called CyberCIEGE conducted at the Naval Postgraduate School. CyberCIEGE is a computer simulation game designed to teach network security and information assurance (IA) concepts to personnel from government and non-governmental agencies.

The research focused on improving cyber-security education by incorporating network traffic analysis into the simulation engine of the CyberCIEGE network security learning game.

The research also identified a subset of available network attacks that were most useful as teaching aides and could be best represented in CyberCIEGE from the broad taxonomy of cyber-attacks available.

B. THESIS SCOPE

The scope of the thesis is divided into three main areas.

1. Taxonomy of Cyber Attacks

Research was conducted on a broad taxonomy of cyber-attacks to identify a subset of attacks that could be identified by a network packet analysis tool. From the study, suitable network and application layer attacks that would make good choices for inclusion in the game's scenarios were investigated.

2. Development of a Network Analysis Tool Simulation in CyberCIEGE

A network analysis tool simulator was developed as part of an extension to the existing CyberCIEGE environment. The existing game engine was extended with the capability to simulate realistic network traffic based on game conditions. This simulated traffic would be viewable by the network analysis tool and allow network-level traffic analysis to be performed by the players.

3. Study on the Effects and Mitigation Measures of Identified Attacks

The study also explored the effects of the identified attacks, the traffic analysis representation of these attacks, and the various possible mitigation measures. New scenarios were developed to represent these attacks. The effectiveness of these representations of attacks in CyberCIEGE was evaluated based on the outcomes from the scenarios. Test cases and expected results were defined for each scenario, with the expected results based on real-world expectations. The results for each scenario were evaluated against the expected results to determine whether the scenario and representations of attacks had been correctly defined and represented.

C. THESIS LAYOUT

This thesis is comprised of the following chapters:

- Chapter I – Introduction. This chapter provides the thesis statement, defines the scope of the thesis, and gives an overview of the chapters.

- Chapter II – Background. This chapter describes the CyberCIEGE game and introduces the components of the game. It discusses the network traffic analysis and presents the capabilities of available traffic analysis tools. Related works on existing network analysis education tools are also discussed.

- Chapter III – Requirement Analysis. This chapter describes the requirements of a network traffic analysis tool and its envisaged usage in CyberCIEGE. The requirements and learning objectives of a game scenario illustrating cyber-attacks and their mitigation measures are described.

- Chapter IV – Design and Development Goal. This chapter describes the design objectives of the network traffic analysis scenario. It includes the scenario’s objectives and expected educational outcomes. The scenario’s briefing and description of the virtual users and assets to be protected are discussed. This chapter also describes the design and development of the network traffic analysis tool extension to the CyberCIEGE.

- Chapter V – Testing. This chapter describes the test strategy and test cases that were conducted in order to verify the new scenario and tool.

- Chapter VI – Recommendations. This chapter provides suggestions on future improvements to the network analysis extension in CyberCIEGE.

- Chapter VII – Conclusion. This chapter summarizes the work accomplished for this thesis and discusses final thoughts on the project.

II. BACKGROUND

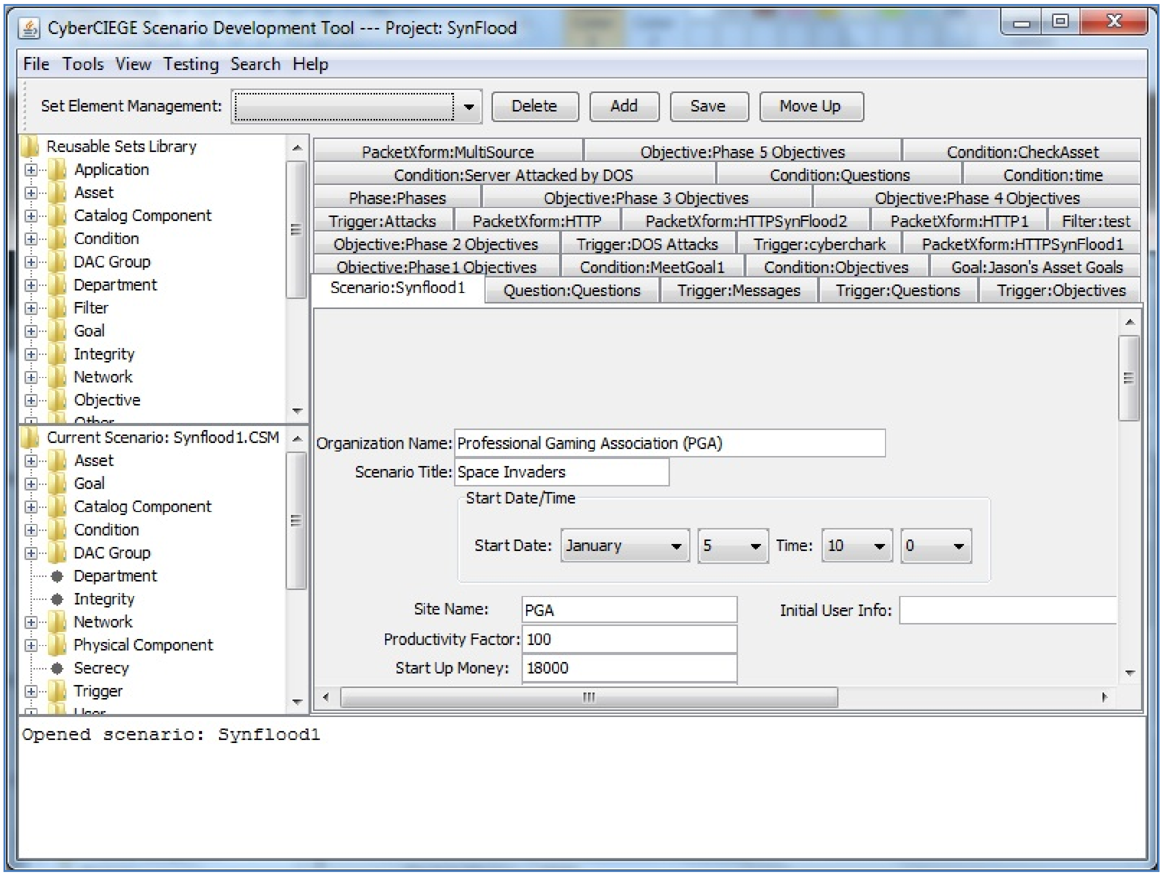
A. CYBERCIEGE

1. Introduction

The CyberCIEGE program is an on-going project by the Center for Information Systems Security Studies and Research (CISR) at the Naval Postgraduate School. It is a video game that employs resource management and simulation to illustrate information assurance concepts using various scenarios. One of its key objectives is to support education and training in computer and network security. Users of the program come from diverse backgrounds in both U.S. government and non-governmental agencies [1].

2. Building Blocks of CyberCIEGE

CyberCIEGE comprises various components, including a unique, real-world, simulation environment, a scenario development tool, a scenario definition language and a video-enhanced encyclopedia [2]. Using the scenario definition language, new scenarios to address different aspects of information assurance or target audiences can be created. The CyberCIEGE game engine interprets and runs the scenarios using the scenario definition language by reading and parsing an external file called the scenario definition file (SDF). The scenario creation process is simplified through the use of the scenario development tool (SDT) which automates the creation of the SDF. Figure 1 shows an illustration of the SDT.



Organization Name: Professional Gaming Association (PGA)

Scenario Title: Space Invaders

Start Date: January 5 Time: 10 0

Site Name: PGA

Initial User Info:

Productivity Factor: 100

Start Up Money: 18000

```
Opened scenario: Synflood1
```

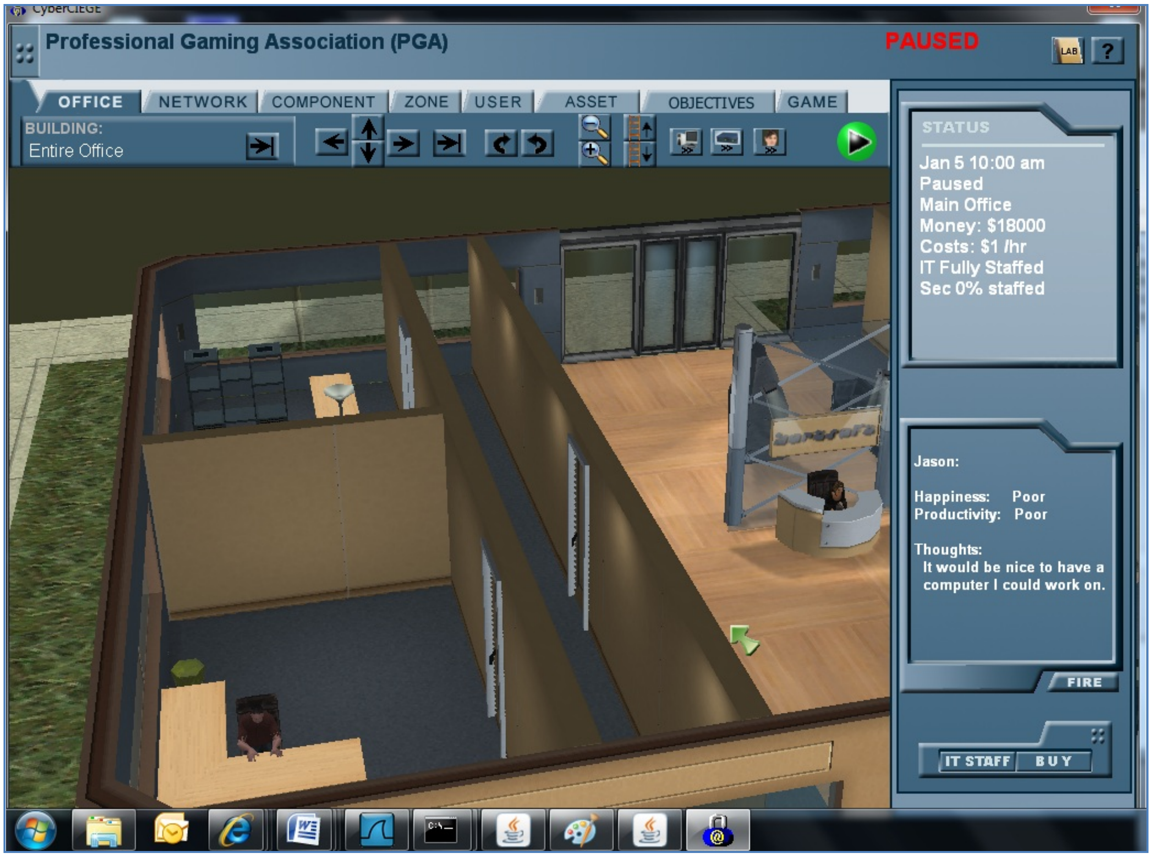
Figure 1. Scenario Development Tool for Building New CyberCIEGE Scenarios

CyberCIEGE is an information technology (IT)/security resource management simulation which requires the player to make decisions and manage a virtual environment using limited resources. The gameplay provides the player with a three-dimensional overhead view of a virtual building/office setting. The player is able to interact with this virtual environment by managing the resources available in the environment, and has the capability to assign new resources. The player must make the correct decisions and provide the necessary resources needed by the virtual users in the game in order to achieve the scenario objectives.

3. Game Play and User Interaction

CyberCIEGE’s gameplay puts the player in charge of an enterprise in a virtual world in which its computer resources must be managed in a secure manner. The player has to make decisions and take responsibility for various aspects of information assurance. These responsibilities include configuring and networking new and existing computer components, making access control decisions, making physical and procedural security choices, and hiring IT support staff. With the given initial budget, the player has to manage the enterprise computer network efficiently and securely and facilitate the virtual users’ ability to accomplish their work goals. These virtual users have to be equipped with the necessary computer components, software, network connections and technical support personnel. Failure to achieve work goals results in monetary losses. The player is also required to create an environment that satisfies the enterprise security policy and protects the assets in accordance with that policy. The player is penalized with monetary losses if the assets are not adequately protected. These losses arise due to the assets being attacked or lost user productivity.

The security choices made by the player will affect the protection level of the assets, which are subjected to attack from simulated vandals, disgruntled employees, professional attackers, incompetent users and acts of nature [3]. Figure 2 shows an illustration of the CyberCIEGE virtual environment.



BUILDING: Entire Office

Jan 5 10:00 am
Paused
Main Office
Money: $18000
Costs: $1 /hr
IT Fully Staffed
Sec 0% staffed

Jason:

Happiness: Poor
Productivity: Poor

Thoughts:
It would be nice to have a computer I could work on.

Figure 2. CyberCIEGE Virtual Environment

4. Benefits of CyberCIEGE

CyberCIEGE provides numerous advantages to educators for the teaching of network security. With the ability to simulate a network in a virtual environment using the game engine, CyberCIEGE eliminates the need to set up a physical environment with an extensive infrastructure. Different networking and end-system components can be introduced into the game without incurring the cost of purchasing them. Students have the opportunity to experiment with different network topologies and systems composed of a heterogeneous mixture of component types and assurance levels via the game.

The richness of the simulation engine and scenario definition language allows complex topics to be presented. Educators can customize their scenarios to suit their educational goals.

B. EXTENSION OF CYBERCIEGE TO INCLUDE NETWORK TRAFFIC ANALYSIS CAPABILITY

CyberCIEGE is an interactive game that simulates realistic scenarios to teach the players about IA concepts. The current game only provides a high-level abstraction of the networked environment in the game scenario, e.g. nodes do not have Internet Protocol (IP) addresses or belong to proper subnets and there is no packet-level network simulation. This study will look into providing the game with a new capability of analyzing network-level traffic as part of the game scenario.

This thesis will develop a new scenario definition file for the CyberCIEGE game. The purpose of the scenario will be to illustrate the importance and usefulness of network traffic analysis in the context of network security. Before the scenario can be written, an understanding of network traffic analysis must be developed. What is meant by network traffic analysis? What is it used for? Why is network traffic analysis important? How is network traffic analysis performed? It is not in the scope of this thesis to completely describe all aspects of network traffic analysis, but rather to focus only on security aspects related to the thesis’s research objective of improving cyber security education. This thesis will provide the basic groundwork upon which the training goals of the scenario will be built, and will allow other new scenarios to be developed as part of future work. The following sections explore the security and traffic analysis concepts that the scenario is intended to teach.

In order to provide a realistic simulation experience to the player, a customized application for the analysis tool will be implemented and integrated with CyberCIEGE. The player will have the ability to view network traffic information details in the graphical display of CyberCIEGE by calling up a network analysis tool, just as he would in the real world. The exact data content and format presented to the player is a principal subject of this research. Based on packer header and payload information, the player can learn about the “anatomy” of network-based cyber-attacks. An actual network analysis tool will be used as reference in the design of the network analysis tool for CyberCIEGE.

C. NETWORK TRAFFIC ANALYSIS AND TOOLS

1. Network Traffic Analysis

Network traffic analysis is the process of intercepting and examining data streams that are flowing across a network in order to deduce information based upon protocol semantics. In general, the greater the number of data packets observed, the more information that can be inferred from the traffic. Based on different situations and needs of the organization, network traffic analysis can be performed in real time, periodically in batches, or after a particular event has occurred (e.g., forensics analysis) to support the following purposes:

- Monitoring and Management. To monitor and detect problems over the network (e.g., routing issues and component failures) or to enhance network performance.
- Security. To detect threats, prevent attacks or analyze in-depth security flaws.
- Information Gathering and Statistics. To obtain any kind of information or statistics that may be of interest to any area other than for security or monitoring and management purposes described above.

In this thesis, only the security aspects of network traffic analysis will be discussed in any detail, as the main focus of the research is on teaching network security. Network traffic analysis is a concern in computer security because important information can be gained from monitoring and analyzing the contents, frequency and timing of network packets. Attackers can use network traffic analysis to conduct a variety of network attacks, such as: observation of sensitive data, a denial-of-service attack, and identity spoofing to disrupt, modify, or steal information from a target system. In contrast, defenders can use it to identify security flaws in the system, detect possible signs of an attack, or mitigate an ongoing attack by attempting to determine the nature of the attack and applying appropriate countermeasures to block further attacks.

The main input source of any network traffic analysis is a collection of packets captured from the network, commonly called the dataset. The dataset is captured and analyzed using a tool called packet sniffer or packet analyzer (also known as network analyzer or protocol analyzer). A packet analyzer is a computer program or a piece of computer hardware that can intercept, “interpret,” and log traffic passing over a network. By “interpret,” we mean that the analyzer can decode each packet's raw (binary formatted) data if required and show the values of various fields in the packet based on the protocols used; as well as analyzing this content according to the appropriate Request For Comment (RFC) or other specification(s). More details of a network analysis tools are described in the next section.

2. Network Traffic Analysis Tools

There are several different network traffic analysis tools in the market; two of the more popular are Tcpdump and Wireshark. These tools capture network packets and interpret the binary in order to display the packet data in human-readable form. In addition to capturing “live” packets off the wire/airwaves, these tools are used to display captured packets from saved files.

a. Wireshark

Wireshark’s graphical user interface allows the user to effectively use the tool with a shorter learning cycle. Available for both UNIX and Windows, Wireshark is able to capture live packet data from a network interface or display previously captured packets that were saved in a packet capture (pcap) binary file.

The effectiveness of the analyzer lies in its capabilities to display packets with very detailed protocol information, and to filter the displayed information based on the user’s criteria. WireShark also has the capability to export packet data into different formats, including Extensible Markup Language (XML)[4].

Using the option to export the packet data to XML, the user can select to export either packet summary information or detailed packet information.

b. Tcpdump

Tcpdump is a command-line tool for capturing the contents of network packets [5]. Similar to Wireshark, it is able to filter network traffic based on expressions that are defined as input parameters. The user also has the option to save captured packets as either text files or pcap formatted files.

D. RELATED WORKS

In addition to CyberCIEGE, there are many other similar simulation systems that have been developed to support education and training in computer and network security. The purpose of this section is to look at how other simulation systems represent and model cyber-attacks. By studying and understanding how other systems design and implement this capability, valuable insights may be gained to help us determine the right level of abstraction for representing an attack model in CyberCIEGE.

Four simulation systems most relevant to this thesis (based on review of their literature) were identified for further study. Each identified system was compared with CyberCIEGE and key differences or similarities found are highlighted. The four simulation systems are described below:

1. Cyber Attack Simulator [6]

A discrete-event simulation model was developed to generate cyber-attack representation and intrusion detection sensor data. This simulation model generates intrusion detection systems (IDS) sensors’ alerts based on the result of cyber-attacks and typical “noise” in the network. Users of the simulation have the capability to model a computer network setup and are able to specify the attacks used in a scenario. A file listing the action generated for each attack and the time the action occurred is created after a simulation is run. Each IDS sensor specified in the network also generates an IDS alert file which is used to test security situational awareness and analysis tools. Key differences between CyberCIEGE and the Cyber Attack Simulator (CAS) are that CAS does not have the capability to simulate attack traffic at the network level and was primarily designed to be used in testing security situational awareness and analysis tools. CyberCIEGE’s design is more flexible and extensible in this aspect.

2. Military Academy Attack/Defense Network (MAADNET)[7]

MAADNET is an educational tool that allows the user to explore network construction, information systems, and information assurance. This simulation-based tool uses a client-server architecture, with the client machine first creating the network topologies and placing the information assurance tools before submitting the scenario to the simulation engine on the server for processing. A key difference between CyberCIEGE and the MAADNET is that real-time player interaction is not available in MAADNET as the player is only given a feedback score based on the simulation engine’s evaluation of the submitted scenario. CyberCIEGE’s simulation is more realistic as it allows real-time player interaction.

3. CyberProtect [8]

CyberProtect is a simulation that was built under contract by the Defense Information Systems Agency (DISA). In this simulation, the role of a cyber-security architect is assigned to the player and the player has to work within a budget to purchase components to defend his network against various forms of cyber-attacks. Players can choose from a wide range of tools to purchase and implement, ranging from firewalls, intrusion detection, access control, antivirus, and encryption products, to end-user training, backup and system redundancy. Once the tools are purchased and implemented, the simulation begins and various types of attacks are generated in the system. There are nine possible forms of attacks, including jamming, viruses, moles, social engineering, packet sniffers, data theft, data modification, flooding and imitation/spoofing. The simulation then provides feedback in the form of a score sheet on the nature and effects of the attack and whether the player was successful in defending his network. A key difference between CyberCIEGE and CyberProtect is that real-time player interaction is not possible in CyberProtect. CyberCIEGE’s simulation is more realistic as it allows real-time player interaction.

4. Information Security War Gaming System (ISWGS) [9]

ISWGS is a tutorial-type simulation that was developed by the National Defense University. The simulation provides in-depth focus on specific attack types and defenses. A key difference between CyberCIEGE and ISWGS is that attacks in ISWGS are portrayed pictorially using a multimedia package only. CyberCIEGE’s simulation is more realistic and interactive.

In conclusion, most of the simulation systems studied are only able to generate very high level abstractions of attack models and do not provide real-time interaction with the players. These limitations prohibit players from delving more deeply into the attacks and using network analysis techniques and tools to learn more about the anatomy of attacks. CyberCIEGE was assessed to be technically more advanced than most of the simulation systems reviewed; hence developing network traffic analysis capability, coupled with network traffic analysis tools, in CyberCIEGE would greatly enhance the usefulness of the system and promote this form of animated security learning.

III. REQUIREMENT ANALYSIS

A. INTRODUCTION

In this chapter, we first review several contemporary cyber-attack taxonomies in order to identify one that provides the best introspection on CyberChark’s completeness. Based on this analysis, two specific attack scenarios were identified for inclusion into CyberCIEGE. Finally, we detailed our selection of a method for modifying CyberCIEGE to include a basic form of network traffic analysis.

B. TAXONOMY OF NETWORK-BASED CYBER ATTACKS

Cyber-attacks are increasingly common, becoming more sophisticated as attackers progressively develop more ingenious methods for exploiting specific attack vectors. In order to help identify and defend against new attacks, a significant body of research surveys the current attack landscape and builds various attack taxonomies. A brief survey of the more prominent and recent taxonomies is described in this chapter.

Chapman [10] proposed a three-tier taxonomy based on the access privileges required for the attacks. The three tiers ranged from “no access” to “user access” to “root access,” and within each tier examples of the attacks and their effects were defined. A limitation of this taxonomy is that the three-tier taxonomy is too general for defining specific subsets of cyber-attacks.

Simmons [11] proposed a cyber-attack taxonomy called AVOIDIT (Attack Vector, Operational Impact, Defense, Information Impact, and Target). Five major classes to characterize the nature of an attack were used, classified as: attack vector, attack target, operational impact, informational impact, and defense. The fifth category, classified as defense, was used to provide the network administrator with information on how to mitigate or remediate an attack. Omission of physical attacks and lack of defense strategies were limitations in their proposed taxonomy.

Kjaerland [12] proposed a taxonomy of attacks based on reported cyber intrusions by commercial and government sectors. The reported data is provided by the Computer Emergency Response Team (CERT), which categorized aspects of cyber intrusions according to “method of operation” (MO). MO refers to the methods used by perpetrators to carry out an attack: “Impact,” “Source,” and “Target” which refer respectively to the effect, source, and victim of the attack. In Kjaerland’s research, attacks were analyzed using facet theory and multidimensional scaling, a technique often used when profiling traditional types of crimes. Kjaerland’s taxonomy focused on the motive of the attacker and contained limitations as it provided only a high level view to the methods of operation [12].

Hansman and Hunt [13] proposed a taxonomy with four unique dimensions that provide a cover network and computer attacks, as well as consistency in language when describing attacks. The first dimension covers the attack vector and the main behavior of the attack. The second dimension allows for classification of the attack targets. Vulnerabilities were classified in the third dimension and payloads were classified in the fourth dimension. Beside the four dimensions described above, a number of further dimensions could be added to enhance the taxonomy, such as cost, damage, propagation and defense dimensions. Hansman mentioned the need of future work to improve classifying blended attacks [13], which was a limitation within their taxonomy.

Mirkovic and Reiher [14] proposed two taxonomies for classifying Distributed Denial of Service (DDoS) attacks and DDoS defenses. The taxonomy of DDoS attacks was categorized by degree of automation, exploited weakness, source address validity, attack rate dynamics, possibility of characterization, persistent agent set, victim type, and impact on victim. These categories examined the means used to prepare and perform the attack (recruit, exploit and infect phases), the characteristics of the attack itself (use phase) and the effect it has on the victim. The taxonomy of DDoS defenses was categorized by activity level, cooperation degree, and deployment location, addressing a specific kind or range of DDoS attacks. The combination of classifying DDoS attacks and defenses within a taxonomy aimed to provide researchers with a better understanding of the DDoS problem; however, the paper focused solely on DDoS rather than general cyber-attacks.

After reviewing the various taxonomies, this thesis selected Hansman’s comprehensive four-dimensional taxonomy [13]. This taxonomy is used to identify suitable attack subsets and models to be represented in CyberCIEGE, as it provides the most holistic view of all the cyber-attacks among the taxonomies considered. Hansman’s taxonomy is discussed in detail in the next section.

C. IDENTIFICATION OF SUITABLE ATTACK SUBSET AND MODELS TO REPRESENT IN CYBERCIEGE

As described previously, Hansman proposed a four-dimensional taxonomy: attack vector, attack target, exploited vulnerabilities, and attack payload and effects [13]. As these four dimensions cover the entire spectrum of computer and network attacks, adaptation of this taxonomy fits our requirement to identify attack subsets and models to represent in CyberCIEGE.

In relation to network-based cyber-attacks, the first dimension covers the protocol layer that the attack utilized; for instance, the layer within the four-layer TCP/IP (transition control protocol/Internet protocol) model. The second dimension covers the target of the attack. The target corresponds to a particular service or asset on a host machine within CyberCIEGE. The third dimension covers the vulnerabilities that were exploited to carry out the attack. The fourth dimension includes the effects of the attack.

Examples of some of the classifications for each of the four dimensions of the proposed taxonomy are presented in Table 1.

Table 1. Classification Examples of the Four-Dimensional Taxonomy

1st Dimension (TCP/IP Layer)	2nd Dimension (Target/Asset)	3rd Dimension (Vulnerabilities)	4th Dimension (Effects)
• Data Link • Network • Transport • Application	• User Passwords • Web Server • Web Application • HTTP Web Applications	• Unencrypted Network Traffic • NetBios Protocol • Unencrypted Network Traffic • HTTP Malformed Packets	• Revealing of Passwords • Spoofing • Session Hijacking • Denial of Services

With this taxonomy, various types of network attacks from different network layers could be easily classified along these four dimensions and evaluated for suitability of representation within the CyberCIEGE environment. To illustrate this methodology, examples of classification for three common network-based attacks are given in Table 2.

Table 2. Classification Examples of Network-based Attack

Attacks	**Layer**	**Target**	**Vulnerability**	**Effect**	**Suitability for representation in CyberCIEGE**
TCP Syn Flood	Transport	Web Server	TCP 3-way Handshake	Denial of Service	Yes
Packet Sniffing	Application	Web Traffic	Unencrypted network packets	Revealing information	Yes
ARP Poisoning	Data Link	ARP cache	Unauthenticated ARP Packets	Denial of Service/ Man-in-the-Middle Attack	No. CyberCIEGE does not represent ARP tables or MAC address

Using the examples in Table 2, we had shown how the four-dimensional taxonomy can be used to identify the types of attacks that are suitable for modeling and representation in CyberCIEGE. Modeling all subsets of attacks is not possible within the scope of this thesis. Therefore, two common forms of attack type were selected for representation and development: Syn Flood and Packet Sniffing, representing attacks at the transport layer and application layer respectively. These two attack types are suitable choices as the components involved in the attacks either have existing representations in CyberCIEGE or can be implemented with minimal changes to the game engine. The exploit techniques use by the attacks can also be illustrated using the information extracted by a packets analysis tool which make the choices suitable for representation in a network traffic analysis scenario.

D. FORMULATION OF SCENARIOS TO MEET TRAINING AND EDUCATION OBJECTIVES

A new CyberCIEGE scenario must be developed to illustrate these two network-based attacks and to provide the player with new educational opportunities to perform network analysis, threat identification and mitigation. From the attack scenario, the player can also learn about the effects of these cyber-attacks and their mitigation measures. The efficacy of these attack representations in CyberCIEGE will be evaluated based on the outcomes from the scenarios. Test cases and the expected results will be defined for each scenario based on real-world expectations. The results of each scenario will be evaluated against the expected results to determine whether the scenario and representations of attacks have been correctly defined and represented. Future studies based on real users' experiences from playing the game scenario can be done to verify that the learning objectives of the scenario have been met.

E. IDENTIFICATION OF A SUITABLE NETWORK ANALYSIS TOOL TO BE MODELED IN CYBERCIEGE

Two options were taken into consideration when deciding on the approach to developing the network analysis tool for use within the CyberCIEGE game. The first option was to integrate an existing network analysis tool, while the second option was to model an existing tool within the CyberCIEGE game environment. Several criteria were taken into consideration when evaluating these two options.

1. Integrating an Existing Tool into CyberCIEGE

The first option considered in the preliminary study was to integrate an existing network analysis tool into CyberCIEGE. Specifically, Wireshark, a popular network analysis tool that is widely used due to its graphical user interface and extensive analysis functionality, was considered. An initial approach to using this option was to provide the player with the ability to start up the Wireshark application from the CyberCIEGE environment with Wireshark running independently of CyberCIEGE.

The advantages of using an existing tool were the ability to leverage existing built-in capabilities and complex functionality without the need to rewrite functions. Further, using Wireshark introduces an actual network analysis tool to the players of CyberCIEGE, thereby increasing their familiarity with such analysis tools.

There were, however, also constraints and disadvantages to using Wireshark as an external application. CyberCIEGE is designed to be a standalone simulation game that gives the player the ability to run the game on a standalone machine after downloading and installing a single package. Having an additional dependent third-party application could possibly introduce configuration issues since the Wireshark application is maintained by an external third party. Using a third-party application would also introduce configuration management issues and security risks as the development team for CyberCIEGE has no control over the application.

Using an external application, the CyberCIEGE game engine will not be able to track the interaction of the player with the tool. Game triggers, which depend on these interactions, cannot be created.

The game engine of CyberCIEGE would require enhancement to provide the capability of generating in-game network traffic packets in a pcap-formatted file that is readable by Wireshark. The game environment would require modification as it is unable to track the current game display relative to the component whose network packets are being displayed. As a result, the camera focus of the game environment would be misleading and a player might be confused by the display.

2. Modeling a Network Analysis Tool Within CyberCIEGE

The second option was to build a network analysis tool within CyberCIEGE. The player would invoke the tool while playing CyberCIEGE and the tool would run within CyberCIEGE. While such an approach brings about limitations to the functionalities of the tools, it has distinct advantages.

The key advantage to modeling a network analysis tool within the CyberCIEGE environment was that the development team would retain full control of the design and development of the tool; there would be no dependency on other third-party applications whose design objectives might differ from those of CyberCIEGE.

Minimal extension to the existing game engine would be needed in order to add the capability of generating in-game network traffic. However, this would require significantly less effort than modifying the game engine to interact seamlessly with an external application and the file format of the network packets would also remain under the control of CyberCIEGE.

The tradeoff for building the tool within the CyberCIEGE environment is that the player will not be able to utilize all of the various complex analysis capabilities of Wireshark because this tool does not model the full functionalities and behavior of Wireshark.

3. Evaluation Outcome

After careful consideration of the options and evaluating the advantages and disadvantage of both, the second option of modeling and developing a network analysis tool within the CyberCIEGE environment was selected for two important reasons. Firstly, this would remove the dependency of CyberCIEGE on a third-party application. The development team of CyberCIEGE would retain control over the design and development of the tool to meet its specific objectives. Secondly, using an actual network analysis tool would require significant development work as the game engine would need to generate network packets in a format readable by the tool.

IV. DESIGN AND DEVELOPMENT GOAL

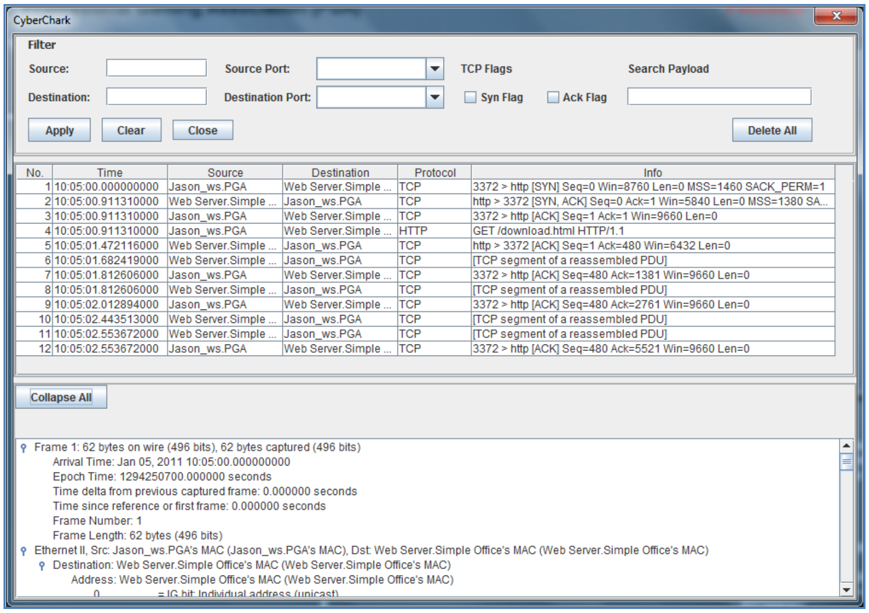
A. NETWORK ANALYSIS TOOL GRAPHICAL USER INTERFACE

The network analysis tool extension in CyberCIEGE was designed to resemble a real-world network analysis tool as closely as possible. A graphical user interface was developed and this interface was designed to provide the player with quick access to both summarized network traffic information and detailed network packet information at a glance.

The network analysis tool extension was developed in Java to maintain compatibility with the game environment.

1. Tool Functionalities

The network analysis tool provides the player with the capability to view both the summary and detailed information of each packet. The tool also provides the capability to filter displayed packets according to a set of fields which the player can define during the game.



No.	Time	Source	Destination	Protocol	Info
1	10:05:00.000000000	Jason_ws.PGA	Web Server.Simple ...	TCP	3372 > http [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM=1
2	10:05:00.911310000	Web Server.Simple ...	Jason_ws.PGA	TCP	http > 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SA...
3	10:05:00.911310000	Jason_ws.PGA	Web Server.Simple ...	TCP	3372 > http [ACK] Seq=1 Ack=1 Win=9660 Len=0
4	10:05:00.911310000	Jason_ws.PGA	Web Server.Simple ...	HTTP	GET /download.html HTTP/1.1
5	10:05:01.472116000	Web Server.Simple ...	Jason_ws.PGA	TCP	http > 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	10:05:01.682419000	Web Server.Simple ...	Jason_ws.PGA	TCP	[TCP segment of a reassembled PDU]
7	10:05:01.812606000	Jason_ws.PGA	Web Server.Simple ...	TCP	3372 > http [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	10:05:01.812606000	Web Server.Simple ...	Jason_ws.PGA	TCP	[TCP segment of a reassembled PDU]
9	10:05:02.012894000	Jason_ws.PGA	Web Server.Simple ...	TCP	3372 > http [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	10:05:02.443513000	Web Server.Simple ...	Jason_ws.PGA	TCP	[TCP segment of a reassembled PDU]
11	10:05:02.553672000	Web Server.Simple ...	Jason_ws.PGA	TCP	[TCP segment of a reassembled PDU]
12	10:05:02.553672000	Jason_ws.PGA	Web Server.Simple ...	TCP	3372 > http [ACK] Seq=480 Ack=5521 Win=9660 Len=0

```
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
    Arrival Time: Jan 05, 2011 10:05:00.000000000
    Epoch Time: 1294250700.000000 seconds
    Time delta from previous captured frame: 0.000000 seconds
    Time since reference or first frame: 0.000000 seconds
    Frame Number: 1
    Frame Length: 62 bytes (496 bits)
Ethernet II, Src: Jason_ws.PGA's MAC (Jason_ws.PGA's MAC), Dst: Web Server.Simple Office's MAC (Web Server.Simple Office's MAC)
    Destination: Web Server.Simple Office's MAC (Web Server.Simple Office's MAC)
        Address: Web Server.Simple Office's MAC (Web Server.Simple Office's MAC)
            0              = IG bit: Individual address (unicast)
```

Figure 3. Graphical User Interface (GUI) of Network Analysis Tool in CyberCIEGE

The fields, which the player can use to define his filter, were proposed based on their usage in a preliminary analysis of network traffic to identify network-based attacks.

The proposed fields were:

- Source and Destination IP Addresses
- Source and Destination Port Numbers
- TCP Flags for Ack and Syn
- Application Layer Payload

Based on the source and destination IP addresses and port numbers, individual user datagram protocol (UDP) and TCP packets can be associated with single sessions. Additionally, the TCP flags filter allows packet filtering based upon session state information which is represented by certain header flags.

Further, a text search capability allows filtering based on the application payload of the network packets.

2. Integration with CyberCIEGE

The network analysis tool interface was developed as a dialog component to be used within the CyberCIEGE game environment. Predefined sets of network packets in XML-formatted files were saved for different types of network traffic. These XML files have placeholders defined in them that are dynamically populated based on the source and destination computer names and domains provided by the game engine during game execution. The XML files are also dynamically updated with realistic game time provided by the game engine.

A new component, PacketXform, was created in the CyberCIEGE game engine. This component defines the source and destination computer name as a function of a particular game scenario’s goals and assets. A new trigger class of PacketXform was also defined in the CyberCIEGE game engine. Using the SDT, we were able to define a trigger that took the PacketXform and a network packets file as parameters. Once activated, the trigger initiates a function that that selects the pre-defined network packets file and reads its XML contents. The function will process the XML contents by replacing the placeholder entries with the appropriate values before appending them to the network packets log of the destination machine. Figure 4 describes the process flow to create a network traffic logs file.

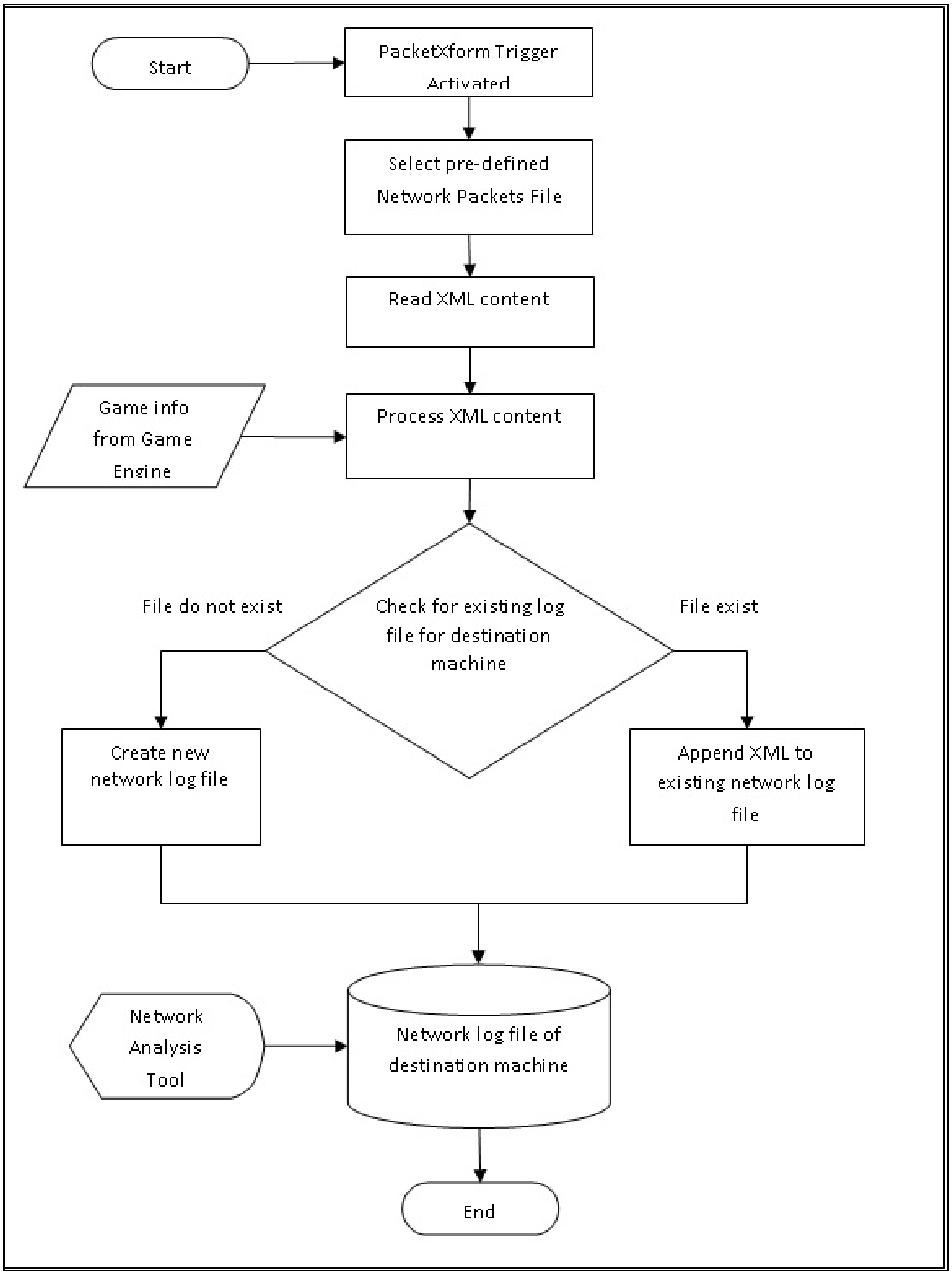

Start
PacketXform Trigger Activated
Select pre-defined Network Packets File
Read XML content
Game info from Game Engine
Process XML content
File do not exist
Check for existing log file for destination machine
File exist
Create new network log file
Append XML to existing network log file
Network Analysis Tool
Network log file of destination machine
End

Figure 4. Flowchart for Creation of Simulated Network Packets

B. MODEL AND DATASETS

1. Types of Attacks

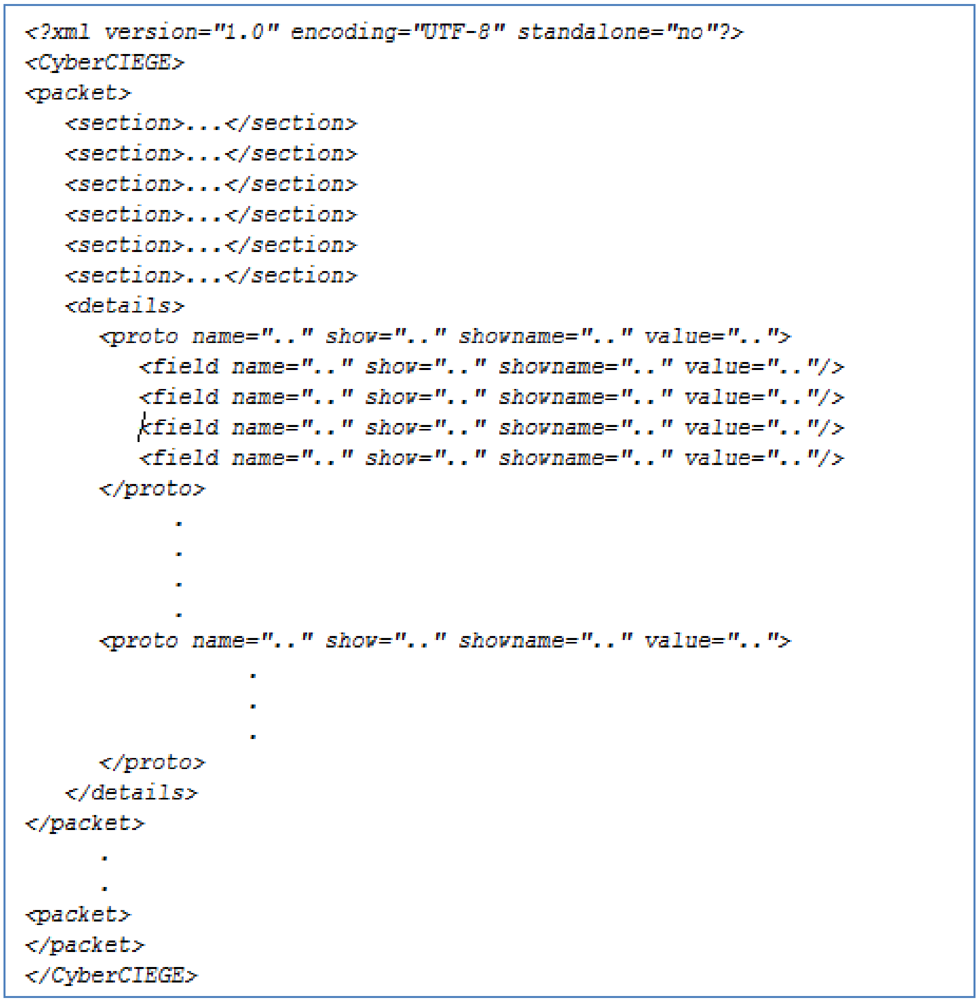
Two network-based attacks were modeled in this thesis and a scenario illustrating these attacks and their mitigation measures was developed.

The first attack modeled is a transport layer attack which attempts to cause denial of service to a Web server through TCP Syn flooding. By exploiting the three-way handshake of the TCP protocol, an attacker could exhaust the resources of a host machine by creating a large number of “half-open” connections. Once the limit of half-open connections is reached, the host would not be able to service requests from legitimate users.

The second attack that was modeled was an application layer attack which involved sniffing an authentication credential over an unencrypted Hypertext Transfer Protocol (HTTP) session. By sending such information over an unsecure channel, the information could possibly be subjected to an eavesdropping attack on the transmission channel or at the host endpoint.

2. XML Structure of Network Packets

Each pre-defined network packets file consists of an XML structure which describes a set of network packets. The structure of the file is illustrated in Figure 5.



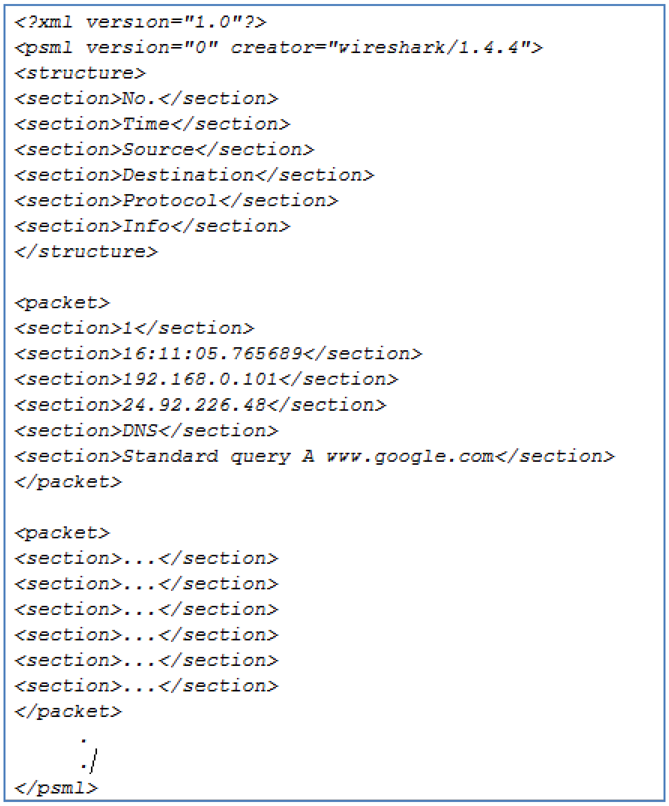
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CyberCIEGE>
<packet>
   <section>...</section>
   <section>...</section>
   <section>...</section>
   <section>...</section>
   <section>...</section>
   <section>...</section>
   <details>
      <proto name=".." show=".." showname=".." value="..">
         <field name=".." show=".." showname=".." value=".."/>
         <field name=".." show=".." showname=".." value=".."/>
         <field name=".." show=".." showname=".." value=".."/>
         <field name=".." show=".." showname=".." value=".."/>
      </proto>
            .
            .
            .
            .
      <proto name=".." show=".." showname=".." value="..">
                  .
                  .
                  .
      </proto>
   </details>
</packet>
      .
      .
<packet>
</packet>
</CyberCIEGE>
```

Figure 5. XML Structure of Network Packets Representation

The structure of the XML packet was designed to resemble the XML packets that could be exported from Wireshark. Wireshark is a network analysis tool that uses pcap-formatted files as the input file. The Wireshark application allows the user to export the displayed packet as either an XML Packet Summary (.PSML) or an XML Packet

Detail (.PDML). A PSML file contains the summary information of the captured packets. The structure of a PSML file exported from Wireshark is shown in Figure 6. A PDML file contains the detailed information of each captured packet. The structure of a PDML file exported from Wireshark is shown in Figure 7.

The structure of the XML file was designed to incorporate both the structures of the PSML and PDML files into a single file for used in CyberCIEGE. With this approach, new datasets of network packets representation could be easily created by exporting their corresponding PSML and PDML files and combining the files. As XML is in human-readable textual format, the XML representation of the network packets could be edited using any text editor. This ease of modification was a key reason for using XML as the representation of network packets in CyberCIEGE instead of a pcap-formatted file.

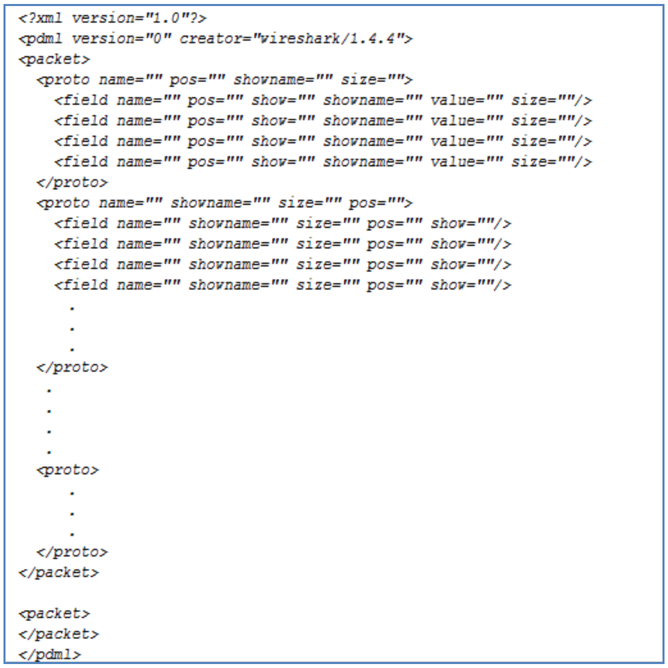


```
<?xml version="1.0"?>
<psml version="0" creator="wireshark/1.4.4">
<structure>
<section>No.</section>
<section>Time</section>
<section>Source</section>
<section>Destination</section>
<section>Protocol</section>
<section>Info</section>
</structure>

<packet>
<section>1</section>
<section>16:11:05.765689</section>
<section>192.168.0.101</section>
<section>24.92.226.48</section>
<section>DNS</section>
<section>Standard query A www.google.com</section>
</packet>

<packet>
<section>...</section>
<section>...</section>
<section>...</section>
<section>...</section>
<section>...</section>
<section>...</section>
</packet>
      .
      .
</psml>
```

Figure 6. Packet Summary XML Structure



```
<?xml version="1.0"?>
<pdml version="0" creator="wireshark/1.4.4">
<packet>
  <proto name="" pos="" showname="" size="">
    <field name="" pos="" show="" showname="" value="" size=""/>
    <field name="" pos="" show="" showname="" value="" size=""/>
    <field name="" pos="" show="" showname="" value="" size=""/>
    <field name="" pos="" show="" showname="" value="" size=""/>
  </proto>
  <proto name="" showname="" size="" pos="">
    <field name="" showname="" size="" pos="" show=""/>
    <field name="" showname="" size="" pos="" show=""/>
    <field name="" showname="" size="" pos="" show=""/>
    <field name="" showname="" size="" pos="" show=""/>
      .
      .
      .
  </proto>
   .
   .
   .
   .
  <proto>
      .
      .
      .
  </proto>
</packet>

<packet>
</packet>
</pdml>
```

Figure 7. Packet Detail XML Structure

3. Representation of Network Packets in CyberCIEGE

Each XML file consists of multiple “packet” nodes which would define the packets for each type of traffic. Within each “packet” node, there are six “section” nodes, which define the Frame Number, Source Address, Destination Address, Source Port, Destination Port, Protocol and Info for each packet. After the six “section” nodes, the “details” node defines the detailed packet information from the data link layer through to the application layer. Each layer’s information is represented by the “proto” node and its “field” children nodes.

C. SCENARIO GOALS

1. Scenario Overview and Layout

The scenario simulates a typical office environment in the commercial sector. The company in this scenario, named “Professional Gamers Association” (PGA), is a well-known developer and publisher of entertainment and educational software. The company is located in Monterey, California and consists of two locations: the main office and a remote office cum data center. Most of PGA’s employees work in the main office, while, due to space constraints, a smaller group is located at the remote office. All the servers are housed in the data center of the remote site. The player of the scenario will assume the role of head of the IT Support and Security Department for PGA. Due to cost-cutting measures at the company, the IT Support and Security Department is given the huge responsibility of managing and protecting the entire IT infrastructure of the company, ranging from the acquisition of computers and network equipment to the deployment and maintenance of security solutions. The player is given an objective in the game briefing that must be met in order to succeed in the game. It is assumed that the player will read the initial briefing, as well as the various user and asset goal descriptions, in order to become familiar with the requirements of the scenario.

2. Narrative of the Scenario

The scenario begins with an initial welcome screen that introduces the player to the PGA scenario. The briefing is intended to give the player a quick overview of the background, current situation, and his initial objectives to get him started. In order to promote active learning and critical thinking, hints will not be given to the players during the initial briefing, but instead revealed progressively during gameplay when he is not making progress or he is not able to complete his objective within a certain time period. The following is the initial briefing to the scenario:

> *Welcome to the Professional Gamers Association. After six years of planning and development, the company is finally almost ready to launch its latest massively multiplayer online role-playing game (MMORPG) “SyberSIEGE”! The product is currently in the final stages of beta testing and the project team is preparing for a full-scale product launch via PGA’s Internet website by end of the year.*
>
> *Sam Bootlicker is the project manager for project SyberSIEGE. He has been a favorite employee of PGA's management for the past two years. Having been awarded "The Best Employee of the Year" recently, he is destined for another promotion if he manages to successfully complete SyberSIEGE in time and launch it online through the company's website by end of the year.*

> *As the head of the IT Support and Security Department, management has requested that you give full support and priority to project SyberSIEGE to ensure the product is launched successfully on the company's website. Management has tasked Sam to help create a new product webpage on the company's Internet website to prepare for SyberSIEGE's launch. Help Sam Bootlicker set up a workstation in his office to connect to the company's Web server located in the remote site's data center to enable him to access and set up a new product webpage.*
>
> *The scenario is divided into several phases. You must complete all objectives of a phase to move to the next phase. Use the OBJECTIVES button in the OFFICE tab to see your objectives for each phase. Press "F1" at any time to view the CyberCIEGE encyclopedia, which includes a "How To" section. Press "k" to view keyboard shortcuts and navigation keys. Click the "OFFICE" tab and the green key "play" button to begin play. Good luck!*

3. Elements of the Scenario

This section describes the main elements that constitute the scenario.

a. Users

CyberCIEGE has two types of game characters which are simulated in a scenario. The first is a user that interacts within the virtual environment and is affected by decisions made by the player during gameplay. The user is typically assigned one or more asset goals that must be accomplished in the scenario. The CyberCIEGE SDT allows a user to be configured to belong to a predetermined department, mandatory secrecy and integrity levels, as well as to one or more Discretionary Access Control (DAC) groups. User trustworthiness, initial training, happiness and productivity levels are some of the variables that can be used in a scenario to reflect the current situation and behavior of the characters, to track whether the player has achieved a certain state, or to trigger an event or action during gameplay.

The second type of game character is a support staff member that is either technical support (helping to keep components available and manage the component configuration settings) or security (e.g., guards). Unlike a user, a support staff member can be working at the beginning of a scenario, or he might be made available for players to hire. Hardware, software, and people skills are variables used to determine the effectiveness of the support staff in dealing with certain aspects of the game, such as physical security and availability of a component. In this scenario, only users are required. A support staff member is not required for achieving the educational goals; hence the scenario will be pre-configured with adequate support staff so as not to affect any of the conditions or variables during gameplay. Table 3 summarizes the attributes required for each character as initially set in the SDF. All numerical attributes are on a scale of 1-100.

Table 3. Game Character Attribute Summary

Character	Department	Asset Goals	Productivity	Happiness
Sam Bootlicker	Projects	Create SyberSIEGE Webpage	90	99
Joe Invidious	Projects	None	50	50
Tina Fuss	Sales	Read Sales Figures	80	80

(1) Sam Bootlicker. Sam Bootlicker is the project manager for project SyberSIEGE. He is tasked by the management to help create a new product webpage on the company’s internet website to prepare for SyberSIEGE’s launch. Therefore, Sam has an asset goal of “Create SyberSIEGE Webpage.” Key attributes of this character are high productivity and a high happiness level. Sam is located in the main office site.

2) Joe Invidious. Joe Invidious is a colleague of Sam Bootlicker. Prior to project SyberCIEGE, they worked closely together on many other projects. After he was promoted to project manager, Sam reassigned Joe to the maintenance team. Joe does not have an assigned computer. His key attributes are low productivity and a low happiness level. Joe is located at the remote office site.

(3) Tina Fuss. Tina Fuss is a senior sales manager from the sales department. She monitors the sales figures daily from the company’s website using an assigned computer; therefore, she has an asset goal of “Read Sales

Figure.” Her key attributes are high productivity and a high happiness level. Tina is located at the remote office site.

b. Assets

Assets are objects or information that are valuable to an organization. In CyberCIEGE, users access assets as part of a goal to be productive and happy. An asset must be appropriately protected while still being available to those that need access. The following sections describe the asset that is defined in the scenario:

(1) PGA Internet Website Information. This is the organization’s main website which contains information about the company and its products. The website has an online store so customers can purchase the latest products online. There are also links to upcoming new products, as well as a customer support site for downloading updates and requesting support. The website is mainly accessible by the public via the Internet except for some pages which are accessible only by authorized staff. For example, a webpage that contains all the sales information on products being sold via the online store is only accessible by authorized users in the sales department.

c. Physical Components

When the player begins this scenario the company Web server is residing in the data center of the remote site. Only Tina Fuss has an assigned computer to access the Web server and read the sales figures.

d. Networks

Some default networks are set up to connect the physical components in the scenario. A Local Area Network (LAN) is set up within the remote office to connect Tina’s workstation to the Web server. A router is also configured in the remote office to allow the Web server to be accessible by the main office users and customers via the Internet.

e. Goals

Goals are associated with users, and are used to specify assets they need to access. Goals determine whether users are able to complete their tasks successfully. If a goal associated with a user is not met, then the user’s productivity and happiness level will drop and affect the company’s bottom line (which is simulated in the form of penalties whereby every hour a certain amount of money is deducted from the player’s available cash). Therefore, in order to meet the objectives of the scenario, the player must provide the necessary components and security protection to the assets to ensure that the user goals are being met. The following are the descriptions of the asset goals in the scenario:

(1) Create SyberSIEGE Webpage. This goal requires read and write access to the PGA Internet Website Information asset to allow Sam Bootlicker to create a new product launch webpage on the Web server. Since Sam has no computer and the asset is located in the remote office data center, the player will need to purchase a workstation and a router to access the Web server via the Internet. The

player will also need to increase the security of the remote access connection to protect the asset.

(2) Read Sales Figures . This goal requires read access to the PGA Internet Website Information asset to allow Tina Fuss from the sales department to access the Web server to read the sales figures. Tina’s goals are already pre-configured to be met as part of the initial scenario requirements. This user illustrates an important IA concept during the later phases of the scenario.

f. Zones

The entire scenario is divided into two zones, the main office zone and the remote site office zone. Since physical security is not part of the educational goals of this scenario, both zones will be pre-configured with adequate physical security controls so that their settings do not affect other variables during gameplay. The zones will be built with receptionists, security guards, card access, surveillance cameras, key locks and photo ID badges for identification, similar to what the real world would have implemented.

g. Conditions and Triggers

In CyberCIEGE, conditions are set in the scenario to check for certain input variables, settings, events or occurrences during gameplay. When these conditions occur, the CyberCIEGE game engine will execute the corresponding triggers associated with these conditions. Triggers are specific game actions that occur in response to these conditions. Examples may include popup messages, tickers, attacks, changes in variables, etc. The conditions and triggers in this scenario are defined in Appendix A.

h. Phases and Objectives

This scenario is divided into five phases. Each phase challenges the player in a specific area of IA and the player will need to demonstrate knowledge of the specific IA issues being tested in order to satisfy the goals depicted in each phase and to proceed to the next phase.

Phase 1 introduces the player to the concept of network traffic analysis and the usage of the network analysis tool (CyberChark). This phase also introduces the player to a specific type of application layer attack (Packet Sniffing). The player will learn the nature of this form of attack and perform the necessary actions to mitigate it. To player is introduced to the usage of the network analysis tool by having to learn to use the tool to extract payload information from the captured network traffic in order to identify account credentials “stolen” (observed in packet traffic) by the attacker.

Phase 2 introduces the player to a specific type of transport layer attack (Syn Flood Attack). The attack will originate from a single attack source and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack.

Phase 3 introduces the player to a variation of the Syn Flood attack wherein the attack will originate from multiple attack sources coming from a single domain and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack.

Phase 4 introduces the player to another variation of the Syn Flood attack wherein the attack will originate from multiple attack sources coming from multiple domains and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack.

Phase 5, the final phase, introduces the player to the final variation of the Syn Flood attack where the attacker uses IP spoofing to formulate a valid IP packet to bypass the firewalls and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack. By the end of this phase, the player will better understand some of the risks associated with connecting to the Internet.

4. Educational Outcomes

Prior to the work completed in conjunction with this thesis there were no available tools in CyberCIEGE to teach and illustrate the importance of network traffic analysis in the context of network security and to validate IA concepts learned and acquired from lessons and textbooks. The development of the scenario and the network traffic analysis tool in this thesis aimed to provide a more realistic and effective training aid to complement lecture-style education in IA. The scenario developed for this thesis is designed to be modular and sequential in approach, such that the players will be introduced to basic concepts first before learning more in-depth concepts as they proceed further into the game. The following sections describe the intended users of this scenario, the educational goals derived from this scenario, and how elements of CyberCIEGE can be used to achieve these educational goals.

a. Intended Users

The intended audience of this scenario can be generalized into two main groups: 1) Users desiring education in network security and 2) Educators or trainers.

(1) Users desiring education. This group is the main audience of the scenario. The Naval Postgraduate School currently uses CyberCIEGE as part of their course syllabus in their Introduction to Computer Security course to introduce and teach concepts on computer and network security via hands-on exercises that reinforce materials presented in lectures or reading assignments [2]. As players have different levels of IA knowledge and experience, CyberCIEGE has scenarios tailored to address different aspects and levels of IA training, helping players to learn and think through each scenario and evaluate impacts on the overall security of the network. In

particular, the scenario developed for this thesis introduces players to the basic concept of network traffic analysis and how to use network tools to conduct in-depth analysis.

(2) Educators or Trainers. The second group using the scenario would be educators or trainers, especially those who teach Information Assurance curricula in various educational institutions and may want to incorporate this game into their courses to enhance student learning. The simulated game environment allows students to explore on their own by trying out various experiments and configurations. The game “adapts” its response/feedback to the player based on his or her actions. The game allows educators or trainers to assess a student’s progress via log generation, and collection and analysis of the actions that the student has taken. The educator can facilitate greater learning by using these results as teaching illustrations. The educator may also use the game for lab exercises to reinforce certain security topics taught during lectures in class.

b. Educational Goals

This scenario is designed with two educational goals: 1) To understand the anatomy of network-based cyber-attacks and 2) To understand the impacts and mitigation measures. The intention is to convey these network security concepts to the players as they execute the game scenario. Players will learn and appreciate how certain network tools can be used to perform network traffic analysis in order to identify a type of network-based cyber-attack or perform in-depth analysis into the packet-level payload data to retrieve useful information. The player can also learn about the effects of these attacks and their mitigation measures.

(1) Anatomy of Network-Based Cyber Attack. Network traffic analysis is an important capability in helping organizations identify and study the nature of network-based cyber-attacks because it is difficult to detect and identify these attacks just by monitoring the behavior of end systems (i.e., client hosts and servers) or analyzing their system logs. Often attacks have already occurred by the time the organization becomes aware of the incidents; so there is a need for real-time traffic analysis capability. An attack may use stealthy methods or normal channels to access the system (e.g., using accounts with sniffed passwords), making detection and identification even more difficult. Hence there is a need to learn more about the analysis process and the tools used to gain important information from monitoring and analyzing the contents, frequency and timing of network packets captured in the system. By understanding the nature of the attacks, organizations can apply the appropriate countermeasures to defend against them.

In CyberCIEGE, a network analysis tool simulator (based on the popular Wireshark packet analyzer) was implemented and integrated with CyberCIEGE. Players now have the capability to view network traffic information details in the graphical display of CyberCIEGE by calling up a network analysis tool. Based on the scenario and generated payload information, the player can analyze and learn more about the anatomy of the attacks. The educational goal is achieved in the scenario when the player is able to employ the network analysis tool and use it to identify, and correct, the presented cyber-attack.

5. Summary

This chapter provided a description of the scenario and its key elements. To achieve the goals in each phase, the player will need to understand the objectives and the needs of the users, and to provide them the necessary components and security protection for the assets. Once all the phases are completed successfully within a certain timeframe, the player is deemed to have “won” the scenario. Otherwise the player is deemed to have “lost” the game and will have to restart and play the scenario again.

The proposed solution to the scenario and verification testing is discussed in the next chapter.

V. TESTING

This chapter describes the scenario testing procedures conducted for this thesis. The testing and verification methodology is explained, followed by detailed descriptions of the test cases and their results.

A. PURPOSE OF TESTING

This scenario is designed with two educational goals: 1) To understand the anatomy of network-based cyber-attacks and 2) To understand the impacts and mitigation measures of the cyber-attacks. As the game progresses in the scenario, information and feedback is provided to the players to help them think, learn, make correct decisions and to guide them through the scenario. Depending on their actions, the scenario will respond with positive feedback to correct actions to encourage the players, or provide immediate negative feedback.

There are two purposes of this testing: 1) To verify that the scenario meets the two educational goals and 2) To verify that the CyberCIEGE game engine behaves as expected to facilitate future regression testing. In order to achieve both purposes, test cases were designed to be incremental to verify the flow of the scenario. Each test case describes a unique situation in the scenario that helps the player learn and achieve the educational goals, as well as the expected behavior and results based on real-world expectations. The scenario was executed according to the test cases and its behavior was observed. If the observed results matched the expected results, the scenario was verified to be correct.

Otherwise, the scenario needed to be modified and tested again until its results were correct.

To verify that the CyberCIEGE game engine behaves as expected to facilitate future regression testing, test procedures were developed by utilizing the game logging function in CyberCIEGE, which logs each event that occurred during the gameplay. After the scenario is played, CyberCIEGE saves the resulting log and it can be replayed automatically without manually repeating the steps from the beginning. These replay logs enabled the test procedures to be repeatedly run against the game engine. For each of the test cases formulated in the next section, two types of replay logs are generated. The first type of replay log is based on the ideal flow when the player performs the expected actions. The second type of replay log is based on the user performing wrong actions, resulting in the attacks.

In each test case, two types of tests were considered. The first type of testing is based on the expected model solution of the game to verify that the game executes correctly according to the design of the scenario. The model solution to the game describes the steps necessary to achieve the objectives of the scenario. The second type of testing is based on expected alternatives or failure conditions. When the players configure the components insecurely or make bad security decisions, the game should respond with negative feedback. During the development of the scenario, it was noted that there were more than one possible solutions to the game. Regardless of the solution chosen, the players will still eventually achieve the same goal according to the design of the scenario.

B. TEST CASES

Two sets of test cases were defined based on the two selected attacks (Syn Flood Attack and Packet Sniffing) described in Chapter III for representation and development in CyberCIEGE. Each test case is organized into the following three subsections:

- Scope of the test - Describes the test procedures to achieve the scenario goals.
- Expected results - Describes the expected scenario behavior that should occur when the player applies the test procedures accordingly or if the player deviates from the solution.
- Actual results – Describes the actual results captured from the execution of the game.

The actual results produced by each of the tests are observed and compare to the expected results to verify that the game responds as expected.

1. Test Case 1: Application Layer Attack

a. Scope of Test Case

Test Case 1 focuses on the basic concept of network traffic analysis by introducing the player to the network analysis tool (CyberChark) and a specific type of application layer attack (Packet Sniffing) under Phase 1, where the attacker (Joe) is able to sniff the victim’s (Sam) login account information via the Internet and use it to access and perform unauthorized modifications to the Web server. Before the application layer attack can occur in the scenario, the player must first set up a computer terminal for user Sam in the main office with an Internet connection to the Web server. Once the attack has occurred, the player will learn more about the nature of this form of attack and perform the necessary actions to mitigate the attack. In CyberCIEGE, there are three possible ways to mitigate this attack. The first method is to establish a Virtual Private Network (VPN) connection between the client and the server. The second method is to implement Secure Socket Layer (SSL) between the client and the server and the third method is to implement One-Time Passwords (OTP) between the client and server. As the third method, OTP, does not facilitate the development of the scenario gameplay to meet the educational goals, the “No One-time Passwords” parameter is configured “true” by default during scenario development to make the Web server application incompatible to support one-time password protocols during game play. This configuration effectively forces the player to use either of the first two methods mentioned above.

To introduce the player to the usage of the network analysis tool (CyberChark), a multiple-choice question is posed to the player after he has successfully mitigated the attack to identify the account credentials used by the victim (Sam). Before he can proceed to the next phase (Phase 2), the player will need to learn to use CyberChark to extract payload information from the captured network traffic in order to correctly identify Sam’s account credentials. Therefore, the player is expected to:

- Purchase a computer workstation and a router, place them in the main PGA office and connect them to the main PGA office LAN and Internet.
- Mitigate the password sniffing attack by configuring SSL encryption between Sam’s workstation and the PGA Web server or configuring a simple VPN between Sam’s workstation and the PGA Web server.
- Use CyberChark to search for “credentials” information under payload search.
- Identify the user account and password information from the credentials found, and answer a multiple choice question correctly.

b. Expected Results

If the player follows the steps to the solution as highlighted in the above paragraph, the scenario will complete Phase 1 of the game and proceed to Phase 2.

If the player does not provide a workstation, a router or network connection to fulfill Sam’s asset goal, Sam’s productivity will drop, reducing the efficiency of the main office, and the player will incur monetary penalties.

If the player does nothing to improve the security of the system after an attack, or does not have enough security measures, the CyberCIEGE game engine will continue to generate insider attacks to compromise the assets.

If the player tries to configure one-time passwords, the CyberCIEGE game engine will notify the player of the incompatibility.

If the player answers incorrectly on the multiple choice question, before proceeding to the next phase the CyberCIEGE game engine will provide help tips and repeat the question every hour until the correct answer is chosen. Table 4 summarizes the tests in Test Case 1.

Table 4. Expected Results of Test Case 1

Test ID	**Description**	**Expected Results**
1a	The player purchases a computer workstation and a router, places them in the main PGA office and connects them to the main PGA office LAN and Internet	Sam will achieve his goal of accessing the SyberSIEGE Web page
1b	The player does not provide a remote workstation or the connection of the workstation to the PGA Web server	Sam will complain and the available budget for the scenario will be reduced
1c	The player does nothing to improve the security of the system after an attack, or does not have enough security measures	The CyberCIEGE game engine will continue to generate insider attacks to compromise the assets

Test ID	**Description**	**Expected Results**
1d	The player configures SSL encryption between Sam’s workstation and the PGA web server	The insider attacks will be mitigated
1e	The player configures the use of one-time passwords between Sam’s workstation and the PGA Web server	The CyberCIEGE game engine will notify the player of the incompatibility
1f	The player identifies the user account and password information from the credentials found and answers a multiple choice question correctly	The scenario will advance to Phase 2
1g	The player is unable to identify the user account and password information from the credentials found and answers a multiple choice question incorrectly	The CyberCIEGE game engine will provide help tips for the player and repeat the question every hour until the correct answer is chosen

c. Actual Results

Table 5 captures the actual results and identifies where the game met the expected results.

Table 5. Actual Results of Test Case 1

Test ID	**Actual Results**	**Meets Expected Results**
1a	Sam achieved his objective of accessing the SyberSIEGE Web page	Yes
1b	Sam complained and the available budget for the scenario was reduced	Yes
1c	The CyberCIEGE game engine continued to generate insider attacks to compromise the assets	Yes
1d	The insider attacks were mitigated	Yes
1e	The CyberCIEGE game engine notified the player of the incompatibility	Yes
1f	The Scenario advanced to Phase 2	Yes
1g	The CyberCIEGE game engine provided help tips for the player and repeated the question every hour until the correct answer was chosen	Yes

As shown in Table 5, the actual test results met the expected results.

2. Test Case 2: Transport Layer Attack

a. Scope of Test Case

Test Case 2 focuses on more advanced usage of CyberChark and introduces the player to a specific type of transport layer attack (Syn Flood Attack) with four different attack variations. Each variation of the attack is simulated in the subsequent phases (starting from Phase 2) in the following order:

In Phase 2, the scenario will simulate an attack originating from a single attack source and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack. The player is also required to answer a few multiple-choice questions correctly to proceed to the next phase. Therefore, the player is expected to:

- Use CyberChark to identify the attack type and attacker host.
- Mitigate the Syn Flood attack by configuring network filters on the network router in the remote office LAN to block the attacker host from accessing the PGA web server via HTTP and HTTPS service from the Internet. If the player configures the network filter to block only HTTP, the attack will continue to persist via HTTPS, and vice versa. If the player configures the network filters to block everyone and only allow Sam’s workstation to access the PGA web server via HTTP and HTTPS, the game engine will generate

a message advising the player that the mitigation method is too drastic to make him rethink his decision.

- Answer multiple choice questions correctly to proceed to the next stage.

In Phase 3, the scenario will simulate an attack originating from multiple attack sources coming from a single domain, targeting the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack. The player is also required to answer a few multiple-choice questions correctly to proceed to the next phase. Therefore, the player is expected to:

- Use CyberChark to identify the attack type and attacker domain.
- Mitigate the Syn Flood attack by configuring network filters on the network router in the remote office LAN to block the entire attacker domain from accessing the PGA web server via HTTP and HTTPS service from the Internet. If the player configures the network filter to block only HTTP, the attack will continue to persist via HTTPS, and vice versa. If the player configures the network filters to block everyone and only allow Sam’s workstation to access the PGA Web server via HTTP and HTTPS, the game engine will generate a message advising the

player that the mitigation method is too drastic to make him rethink his decision.

- Answer multiple choice questions correctly to proceed to the next stage.

In Phase 4, the scenario will simulate an attack originating from multiple attack sources coming from multiple domains and targeting the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack. The player is also required to answer a few multiple-choice questions correctly to proceed to the next phase. Therefore, the player is expected to:

- Use CyberChark to identify the attack type and the various attacker domains and sources.
- Mitigate the Syn Flood attack by configuring network filters on the network router in the remote office LAN to block all hosts except for Sam’s workstation from accessing the PGA Web server via HTTP and HTTPS service from the Internet. If the player configures the network filter to block only HTTP, the attack will continue to persist via HTTPS, and vice versa.
- Answer multiple choice questions correctly to proceed to the next stage.

In Phase 5 (final phase), the scenario will simulate an attack where the attacker uses IP spoofing to formulate a valid IP packet to bypass the firewalls and target the HTTP/HTTPS service of the Web server to cause a denial of service. The player is required to perform more detailed analysis using CyberChark to identify the nature of the attack and perform appropriate actions to mitigate this attack. In this Phase, another user, Tina, is introduced into the scenario. Tina is located in the remote office. She has a “Read Sales Figures” goal and needs to access the PGA Web server via the remote office LAN. Due to IP spoofing from the Internet, the availability of the web server would be low and both Sam and Tina would not be able to achieve their goals. In order to complete the objectives of this phase, the player will need to assess the situation and adopt the best approach, which is to filter all HTTP and HTTPS traffic coming from the Internet to stop the attacks. Although Sam will not be able to access the Web server anymore to achieve his goal, this approach will still allow Tina to meet her goals and avoid disruptions to existing operations, which is also what would have happened in a real-world situation. The player is also required to answer a few multiple-choice questions correctly to win and complete the game. Therefore, the player is expected to:

- Use CyberChark to identify the attack type and spoofed IP traffic.
- Mitigate the Syn Flood attack by configuring network filters on the network router in the remote office LAN to block all hosts from accessing the PGA Web server via HTTP and HTTPS service from the Internet.
- Answer multiple choice questions correctly to complete and win the game.

b. Expected Results

In Phase 2, 3 and 4, if the player follows the steps to the solution as highlighted in the above paragraph, the scenario will complete the current phase of the game and proceed to the next phase. If the player does nothing to improve the security of the system after an attack, or does not have enough security measures, the attack will continue to persist, causing the availability of the Web server to be low, and Sam will not be able to achieve his goal.

In Phase 5, if the player follows the steps to the solution as highlighted above, the scenario will complete Phase 5 of the game and end the game. If the player does nothing to improve the security of the system after an attack, or does not have enough security measures, the attack will continue to persist and cause the availability of the Web server to be low. Tina will not be able to achieve her goal.

From Phase 2 to Phase 5, if the player answers incorrectly on the multiple choice questions, before proceeding to the next phase, the CyberCIEGE game engine will repeat the question until the correct answer is chosen.

Table 6. Expected Results of Test Case 2

Test ID	Description	Expected Results
Phase 2		
2a	The player does nothing to improve the security of the system after an attack, or does not have enough security measures	The attack will persist, causing the availability of the Web server to be low, and Sam will not be able to achieve his goal
2b	The player configures network filters on the network router in the remote office LAN to block the attacker host from accessing the PGA web server via HTTP and HTTPS service from the Internet	The availability of the Web server will become high again and Sam will be able to achieve his goal of accessing the SyberSIEGE Web page
2c	The player configures the network filters to block everyone except Sam's workstation to access the PGA Web server via HTTP and HTTPS,	The game engine will generate a message to advise the player that the mitigation measure is too drastic and make him rethink his

Test ID	**Description**	**Expected Results**
		decision.
2d	The player configures the network filter to block only either HTTP or HTTPS	The attack will persist
2e	The player answers the multiple choice questions correctly	The scenario will advance to Phase 3
Phase 3		
3a	The player does nothing to improve the security of the system after an attack, or does not have enough security measures	The attack will persist, causing the availability of the Web server to be low and Sam will not be able to achieve his goal
3b	The player configures network filters on the network router in the remote office LAN to block the entire attacker domain from accessing the PGA Web server via HTTP and HTTPS service from the Internet	The availability of the web server will become high again and Sam will be able to achieve his goal of accessing the SyberSIEGE Web Page
3c	The player configures the network filters to block everyone, only allowing Sam's workstation to access the PGA	The game engine will generate a message advising the player that

Test ID	**Description**	**Expected Results**
	Web server via HTTP and HTTPS	the mitigation measure is too drastic and making him rethink his decision
3d	The player configures the network filter to block only either HTTP or HTTPS	The attack will persist
3e	The player answers the multiple choice questions correctly	The scenario will advance to Phase 4
Phase 4		
4a	The player does nothing to improve the security of the system after an attack, or does not have enough security measures	The attack will persist, causing the availability of the Web server to be low, and Sam will not be able to achieve his goal
4b	The player configures network filters on the network router in the remote office LAN to block all hosts except for Sam's workstation from accessing the PGA Web server via HTTP and HTTPS service from the Internet	The availability of the Web server will become high again and Sam will be able to achieve his goal of accessing the SyberSIEGE Web page

Test ID	**Description**	**Expected Results**
4c	The player configures the network filter to block only either HTTP or HTTPS	The attack will persist
4d	The player answers the multiple choice questions correctly	The scenario will advance to Phase 5.
Phase 5		
5a	The player does nothing to improve the security of the system after an attack, or does not have enough security measures	The attack will persist, causing the availability of the Web server to be low and both Sam and Tina will not be able to achieve their goals
5b	The player configures network filters on the network router in the remote office LAN to block all hosts from accessing the PGA Web server via HTTP and HTTPS service from the Internet	The availability of the web server will become high again. Sam will not be able to achieve his goal, but Tina will still be able to achieve her goal of reading the sales figures
5c	The player answers the multiple	The scenario will

Test ID	**Description**	**Expected Results**
	choice questions correctly	end and the player wins

c. Actual Results

Table 7 captures the actual results and identifies where the game met the expected results.

Table 7. Actual Results of Test Case 2

Test ID	**Actual Results**	**Meets Expected Results**
Phase 2		
2a	The attack continued to persist and caused the availability of the Web server to be low. Sam was not be able to achieve his goal	Yes
2b	The availability of the Web server became high again and Sam was able to achieve his goal of accessing the SyberSIEGE Web page	Yes
2c	The game engine generated a message to advise the player that the mitigation measure was too drastic	Yes
2d	The attack continued to persist	Yes
2e	The Scenario advanced to Phase 3	Yes

Test ID	**Actual Results**	**Meets Expected Results**
Phase 3		
3a	The attack continued to persist and caused the availability of the Web server to be low. Sam was not be able to achieve his goal	Yes
3b	The availability of the Web server became high again and Sam was able to achieve his goal of accessing the SyberSIEGE Web page	Yes
3c	The game engine generated a message to advise the player that the mitigation measure was too drastic	Yes
3d	The attack continued to persist	Yes
3e	The Scenario advanced to Phase 4	Yes
Phase 4		
4a	The attack continued to persist and caused the availability of the Web server to be low. Sam was not be able to achieve his goal	Yes
4b	The availability of the Web server became high again and Sam was able to achieve his	Yes

Test ID	Actual Results	Meets Expected Results
	goal of accessing the SyberSIEGE Web page	
4c	The attack continued to persist	Yes
4d	The scenario advanced to Phase 5.	Yes
Phase 5		
5a	The attack continued to persist and caused the availability of the Web server to be low. Both Sam and Tina were not be able to achieve their goals	Yes
5b	The availability of the Web server became high again. Sam was not able to achieve his goal, but Tina was still able to achieve her goal of reading the sales figures	Yes
5c	The scenario ended and the player won	Yes

As shown in Table 7, the actual test results met the expected results.

C. SUMMARY

The results from the test cases developed for this thesis verified that the scenario achieved the educational goals and also validated that the feedback provided by CyberCIEGE game engine is commensurate with real-world implementations. The actual results from the testing matched the expected results.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS

A. RECOMMENDATIONS FOR FURTHER STUDY

This chapter describes recommendations for further study. The chapter is separated into two sections. The first section describes possible future extensions to the CyberCIEGE network traffic analysis tool, and the second section discusses areas that can be developed in future CyberCIEGE scenarios.

1. Recommendations for Simulated Network Analysis Tool

a. XML Parsing

The CyberCIEGE network traffic simulation functions use XML-based flat files as input for simulating network traffic packets. The current implementation uses the Java’s Document Object Model (DOM) specification for representation and parsing of the XML data from the input files. The DOM specification for managing XML data is resource intensive and requires a long processing time for large files. An alternative approach would be to use the Simple Application Programming Interface (API) for XML (SAX) specification.

A DOM specification XML parser creates a tree-based representation of the XML data and provides an object-oriented structure of the data, which facilitates ease of navigation between nodes and sub-nodes and helps to simplify the manipulation of the data. Significant processing time, however, is needed as it has to read the entire XML data into memory in order to create the hierarchical structure of the XML data. A test conducted to obtain the approximate amount of time needed to process the XML data for a varying number of packets showed that an overhead of about 18 percent of the processing time was needed to parse the XML. The test result is summarized in Table 8.

Table 8. Time Taken to Generate Simulated Network Packets

Number of Packets	**File Size (KB)**	**Time Taken to Parse XML (ms)**	**Total Time Taken (ms)**	**Percentage of Total Time**
5	46	84	451	18.6%
10	92	194	999	19.4%
15	137	257	1384	18.6%
20	183	343	1814	18.9%
25	229	433	2312	18.7%
30	275	503	2766	18.1%
35	321	600	3422	17.5%
40	367	668	3649	18.3%
45	413	744	4198	17.7%
50	458	840	4756	17.7%

In comparison, a SAX parser allows sequential reading of an XML input file as it uses a streaming interface and does not need to create an internal representation of the XML data in memory. However, the SAX parser is event-based driven and callback functions that handle the events have yet to be developed. This will require additional development efforts. Using this approach can potentially reduce the processing time needed for generating the simulated network packets.

b. Simulating Network Packets

Currently a process to generate the simulated network packets is started when an event is triggered during the gameplay in CyberCIEGE. As the process runs in the same thread as the game engine, a short pause in the game is experienced if the number of simulated packets is large. In this section, two approaches of addressing this delay are identified as possible avenues of further work.

(1) Multi-Threading. When an event occurs and triggers the generation of network packets, a separate thread can be created to run the packet generation process. A second thread will minimize the pause in the game as the game engine is able to continue running in its original thread. However, attention needs to be placed on addressing the synchronization of the game environment with the packet generation process. If a player attempts to access the packet log file before the packet generation process is completed, a splash screen can be used to pause the game while waiting for the process to be completed. Upon completion of the process, the game engine will allow the player to proceed.

(2) Preloading of Network Packet Template Files. The generation of network packets requires reading of XML-based template files. As the content of the files are static, they can be read into memory before the game starts. This will eliminate the processing time needed for reading the template files during runtime.

c. Filter Criteria

Additional filtering criteria can be added to CyberCHARK to allow the player other packet filtering and matching options. The filtering options for the current development were designed to allow the player the ability to easily identity TCP packets and TCP Syn flooding network attacks. New attack traffic can be produced for the game, and filter criteria suitable for identifying such attacks would have to be developed. To further increase the educational value of the game, providing an advanced player with filtering expressions based on multiple criteria will also be beneficial.

d. Additional Features

Other potential features that can be added to CyberChark include TCP stream analysis and a protocol statistic summary. TCP stream analysis will be useful in identifying and showing the TCP conversations between two hosts. A summary of the protocol statistic showing the numbers and types of packets being transmitted will aid the user in identifying the protocols of the packets captured. The development efforts required to implement these new capabilities will be not be significant as the input data can be extracted from the existing simulated network packets, so just the development of the functions to analyze and display the information is required. This would not require an extensive redesign of the game engine.

2. Recommendation for Traffic Analysis Scenarios

a. Enhancement to Existing Question Form

The current question form available in CyberCIEGE only allows players to choose one answer from a pre-formatted set of multiple-choice answers. It is possible that a player may manage to choose the correct answer without actually understanding it through the process of guessing, or by elimination by repeatedly replaying the scenario. Furthermore, for certain question types, using a multiple-choice format may not be an ideal approach for educators to assess the player’s understanding. Additionally, multiple-choice does not allow CyberCIEGE to adapt to the responses as there could be more than one correct answer. Hence, to help improve the player’s learning experience and allow educators to better assess the player’s understanding, two enhancements to the existing question form were proposed:

(1) Allow players to select more than one correct answer from the set of multiple-choice answers.

(2) Allow players to manually input the answer via the keyboard for certain question types that require “fill-in-the-blanks,” so that players cannot easily guess the answer. For this enhancement, only questions that would result in only one possible single and exact word answer (e.g., guessing a password used by a user as described in the password sniffing attack scenario developed in this thesis) would be suitable because otherwise it would be technically difficult to develop CyberCIEGE to automatically “grade” free-form responses so that the gameplay could advance. However, future work could

further develop CyberCIEGE scenarios to incorporate lab exercise, quiz or test formats. This would allow educators to make use of such scenarios to better assess individual student’s learning and grade him based on his submitted results in the lab exercise, quiz or test. We leave these alternatives to future work.

b. Inclusion of IP Addresses and Media Access Control (MAC) Addresses Assignment for Network and Computer Equipment

Currently, CyberCIEGE only provides a high-level abstraction of the networked environment in the game scenario, e.g., nodes do not have IP addresses or MAC addresses, or belong to proper subnets. Certain network security concepts and cyber-attacks such as address resolution protocol (ARP) poisoning cannot be illustrated, represented and modeled in CyberCIEGE without including these additional parameters. Furthermore, the current game’s firewall filtering rules are based only on filtering domain names and hostnames, which is not a true representation of the functionalities of a firewall in the real world. A firewall in the real world would be able to filter by IP addresses and specific ports, but not by domain names and hostnames. Hence, we envision future enhancements to the CyberCIEGE engine to include IP addresses and MAC address assignments for the network, and computer equipment to represent more advanced capabilities and attacks in the game scenario. Further studies could be conducted to better model the firewall filtering in CyberCIEGE to provide a more accurate and realistic representation. Further research will also need to be conducted to determine if any other parameters are required for full implementation in CyberCIEGE.

c. Inclusion of New Equipment Type and Other Network Abstractions

Additional equipment type and network abstractions could be added to CyberCIEGE to enhance learning and allow more advanced security topics to be taught by educators. For example, CyberCIEGE does not model an IDS as part of the computer equipment or software simulated in the game. An IDS is a device or software application that passively monitors the network and system for malicious activities or policy violations and produces reports for further analysis and follow up. IDS' form an important part of the security infrastructure of nearly every organization. Incorporating and simulating IDS' into game scenarios would permit CyberCIEGE to incorporate additional network security topics and concepts. Other examples would be to include the network abstraction for a Domain Name Server (DNS) to model DNS attacks and the addition of a Mail Transfer Agent (MTA) to model spam. There are entire classes of attacks using DNS or against the DNS, such as DNS cache poisoning which could be simulated in CyberCIEGE and further illustrated with CyberChark.

Such advanced concepts in CyberCIEGE would enhance the teaching value for educators as well as the learning value for students. Further research is needed to determine if any other components are required for representation within CyberCIEGE.

d. User Studies

The newly developed game scenario has not been played in a learning environment by students. It would be beneficial to have the intended audience, such as those taking network security-related courses, play the scenario. With actual feedback from users based on their experience in playing the scenario, additional insights may be obtained and this would be useful for enhancing the scenario and providing additional educational value.

A possible means of quantitatively measuring the educational efficacy of the scenario can be done by having the students answer questions regarding the network security concepts that will be brought up in the scenario before the students have actually played the scenario. A similar set of questions would be given to the same students after they have completed the scenario and a gauge of the effectiveness of the scenario can then be obtained by comparing the responses to the two sets of questions.

VII. CONCLUSION

A. ANALYSIS OF IMPLEMENTATION AND SCENARIO DEVELOPMENT

This thesis identified a four-dimensional taxonomy of network-based cyber-attacks in order to identify attacks suitable for representation in CyberCIEGE. This taxonomy provides comprehensive coverage of existing cyber-attacks as well as new and evolving attacks. The research assesses the cyber-attacks for their suitability to be represented in CyberCIEGE based on the characteristics of the attacks. Using this taxonomy, two sets of cyber-attacks were identified as candidates for representation within a CyberCIEGE game scenario.

A new scenario focusing on network-based attacks and their mitigation measures was created for this thesis. An extension to the CyberCIEGE game was designed, developed, and tested. This extension, dubbed “CyberChark,” provides the player with network traffic analysis capabilities similar to those available in existing real-world tools. The new scenario exercises a student’s traffic analysis abilities by requiring players to identify the anatomy of two particular cyber-attacks by using CyberChark during game play.

The new scenario introduces the player to some common network-based attacks and the anatomy of these attacks. By requiring the player to make effective decisions to mitigate the attacks in order to achieve his or her goals, the player is taught possible mitigation measures to common attacks and the effects and trade-offs of these measures.

In conclusion, this thesis achieved its research goal of contributing to cyber-security education by including network traffic analysis into the simulation engine of the CyberCIEGE network security learning game, as well as providing the following benefits:

- A comprehensive taxonomy of attacks for future analysis and reference
- A framework for developing new simulation models for analysis and training, and
- New coursework for training and education requirements in information assurance and network security.

APPENDIX A. LIST OF GAME CONDITIONS AND TRIGGERS

Table 9 below shows a list of the game conditions and triggers developed in the scenario and a brief description for each item.

Table 9. List of Game Conditions and Triggers

S/No	Trigger/Condition	Description
	Conditions	
1.	CheckSSL	• Condition that checks if the player has configured SSL between a particular user and his/her asset goal • Used in the scenario to generate the correct user network traffic information (HTTP or SSL) for display and analysis in CyberChark
2.	CheckSSLFiltered	• Condition that checks if an asset can be reached via a given network through a software filter (SSL) • Used in the scenario to generate the correct DoS network traffic information (SSL) for display and analysis in CyberChark
3.	CheckHTTPFiltered	• Condition that checks if an asset can be reached via a given network through a software filter (HTTP) • Used in the scenario to generate the correct DoS network traffic information (HTTP) for display and analysis in CyberChark

S/No	Trigger/Condition	Description
	Conditions	
4.	CheckSSLFiltered1	• Condition that checks if the player has configured a particular software filter (SSL) in the filtering rules to allow or deny one or more hosts or domain • Used in Phase 2 and Phase 3 of the scenario to check if the player has configured too drastic filtering rules in order to advise the player and allow him to progressively advance through the scenario
5.	CheckHTTPFiltered1	• Condition that checks if the player has configured a particular software filter (HTTP) in the filtering rules to allow or deny one or more hosts or domain • Used in Phase 2 and Phase 3 of the scenario to check if the player has configured too drastic filtering rules in order to advise the player and allow him to progressively advance through the scenario
6.	SamAccessWebSvr	• Condition that checks if Sam is able to reach an asset goal • Used in the scenario to generate the correct network traffic information (HTTP) for display and analysis in CyberChark
7.	TinaAccessWebSvr	• Condition that checks if Tina is able to reach an

S/No	Trigger/Condition	Description
	Conditions	
		asset goal • Used in Phase 5 to check if the player has adopted the correct mitigation measure to block all Internet traffic in order to stop the syn flood attack and allow Tina to continue to meet her goal.
8.	SamProductivity	• Condition that measures the current productivity level of Sam against a test value • Used in the scenario to check if Sam has met his objectives for each phase
9.	TinaProductivity	• Condition that measures the current productivity level of Tina against a test value • Used in the scenario to check if Tina has met her objectives for phase 5
10.	Reg1	• Condition that measures a register value • Used in conjunction with Question1 trigger to store the selected answer
11.	OneHour	• Condition that measures if one hour has elapsed from the beginning of each phase • Use in the scenario to control the flow of attack and message triggers in each phase
12.	ServerAttacked	• Condition that checks if a specific asset has been attacked • Used from Phase 2 to Phase 5 to check if the

S/No	Trigger/Condition	Description
	Conditions	
		player has mitigated the Syn Flood DOS attack in each phase
13.	InsiderAttack	• Condition that checks if a specific asset has been attacked • Used in Phase 1 to check if the player has mitigated the insider attack
	Triggers	
14.	Insider	• Trigger that generates an Insider Hacking Attack • Used in Phase 1 to cause Joe to maliciously modify the SyberSIEGE launch page using Sam's credentials obtained by performing a password sniffing attack from the Internet
15.	DOS	• Trigger that generates a Denial of Service (DOS) Flood Attack • Used from Phase 2 to Phase 5 to simulate a Syn Flood DOS attack from the Internet via HTTP or SSL
16.	HTTP Login	• Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form • Used in Phase 1 to simulate a HTTP login network traffic in CyberChark
17.	SSL Login	• Trigger that appends a given network packet

S/No	Trigger/Condition	Description
	Conditions	
		sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form • Used in Phase 1 to simulate a HTTPS login network traffic in CyberChark
18.	One Source One Domain HTTP	• Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form • Used in Phase 2 to simulate HTTP syn flood attack network traffic in CyberChark coming from a single source within a single domain
19.	One Source One Domain HTTPS	• Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form • Used in Phase 2 to simulate HTTPS syn flood attack network traffic in CyberChark coming from a single source within a single domain
20.	Multi Source One Domain HTTP	• Trigger that appends a given network packet sample to the packet log associated with a given component after

S/No	Trigger/Condition	Description
	Conditions	
		transforming component names as defined in a PacketXform form - Used in Phase 3 to simulate HTTP syn flood attack network traffic in CyberChark coming from multiple sources within a single domain
21.	Multi Source One Domain HTTPS	- Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form - Used in Phase 3 to simulate HTTPS syn flood attack network traffic in CyberChark coming from multiple sources within a single domain
22.	Multi Source Multi Domain HTTP	- Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form - Used in Phase 4 to simulate HTTP syn flood attack network traffic in CyberChark coming from multiple sources and multiple domains
23.	Multi Source Multi Domain HTTPS	- Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component

S/No	Trigger/Condition	Description
	Conditions	
		names as defined in a PacketXform form - Used in Phase 4 to simulate HTTPS syn flood attack network traffic in CyberChark coming from multiple sources and multiple domains
24.	Spoofed HTTP	- Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form - Used in Phase 5 to simulate HTTP syn flood attack network traffic in CyberChark coming from a spoofed user (Sam)
25.	Spoofed HTTPS	- Trigger that appends a given network packet sample to the packet log associated with a given component after transforming component names as defined in a PacketXform form - Used in Phase 5 to simulate HTTPS syn flood attack network traffic in CyberChark coming from a spoofed user (Sam)
26.	Update Attacker Profile	- Trigger that associates the given names with the attacker's computer and the domain from which the attack occurs. These names are used when processing network filters - Used from Phase 2 to

S/No	Trigger/Condition	Description
	Conditions	
		Phase 5 to update the computer name and domain name of the attacker to simulate different variations of the Syn Flood DOS Attack network traffic information for analysis in CyberChark
27.	User Filters Too Drastic	• Trigger that generates a message to inform the player based on condition CheckHTTPFiltered1 or CheckSSLFiltered1 • Used in Phase 2 and Phase 3 to generate a message to advise the player of his/her drastic action if the player attempts to block all HTTP or HTTPS traffic from the Internet except Sam's workstation using the network filter
28.	Guess Password	• Trigger that launches a multiple choice question for the player to select an answer • Used in Phase 1 to ask the player for the correct password credential used by Sam to log in to the PGA Web Server
29.	Question1	• Trigger that launches a multiple choice question for the player to select an answer, which is stored in Reg1 • Used after the end of each Phase to test the player's understanding of the security topics related to each phase. More than one question

S/No	Trigger/Condition	Description
	Conditions	
		may be asked

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006). *Cyber Security Training and Awareness Through Game Play.* Monterey, CA: Naval Postgraduate School.

[2] Irvine, C. E., Thompson, M. F., & Allen, K. (2005). CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness. *Federal Information Systems Security Educators' Association Conference.* North Bethesda, MD.

[3] Irvine, C. E., Thompson, M. F., & Allen, K. (2005). CyberCIEGE: An Extensible Tool for Information Assurance. *CISSE Conference.*

[4] Lamping, U., Sharpe, R., & Warnicke, E. (n.d.). *Wireshark User's Guide for Wireshark 1.7.* Retrieved 2011 йил 23-10 from Wireshark.org: http://www.wireshark.org/download/docs/user-guide-a4.pdf

[5] *tcpdump.org*. (2010). Retrieved 2011 25-October from http://www.wireshark.org

[6] Kuhl, M. E., Kistner, J., Costantini, K., & Sudit, M. (2007). Cyber Attack Modelling and Simulation for Network Security Analysis. *Proceedings of the 2007 Winter Simulation Conference.*

[7] C A Carver, J. R. (2002). *Military Academy Attack/Defense Network.* 3rd Annual IEEE Information Assurance Workshop.

[8] DOD. (2010). *CyberProtect*. From CyberProtect: http://iase.disa.mil/eta/cyber-protect/launchpage.htm

[9] Saunders, J. H. (2001). *The Case for Modeling and Simulation of Information Security*. From http://www.johnsaunders.com/papers/securitysimulation.htm

[10] Chapman, I. M., Leblanc, S. P., & Partington, A. (2011). Taxonomy of Cyber Attacks and Simulation of Their Effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium* (pp. 73 - 80). Boston, Massachusetts: Society for Computer Simulation International.

[11] Kjaerland, M. (Oct 2005). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers and Security* , 522-538.

[12] Simmons, C., Shiva, S., Dasgupta, D., & Wu, Q. (August 2009). *AVOIDIT: A Cyber Attack Taxonomy.* Memphis: University of Memphis.

[13] Hansman, S., & Hunt, R. (2003). A Taxonomy of Network and Computer Attack Methodologies. Christchurch, New Zealand: Department of Computer Science and Software Engineering, University of Canterbury.

[14] Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. *SIGCOMM Computer Communication Review , 34* (2), 39 - 53.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Victor Piotrowski
   National Science Foundation
   Arlington, Virginia, State

4. Sue Fitzgerald
   National Science Foundation
   Arlington, Virginia

5. George Bieber
   Office of the Secretary of Defense
   Washington, DC

6. Peggy Maxson
   Department of Homeland Security
   Washington, DC

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

8. Dr. Robert Beverly
   Naval Postgraduate School
   Monterey, California

9. John D. Fulp
   Naval Postgraduate School
   Monterey, California

10. Michael F. Thompson
    Naval Postgraduate School
    Monterey, California

11. Prof. Yeo Tat Soon
    Director, Temasek Defence System Institute
    Singapore

12. Tan Lai Poh
    Senior Manager, Temasek Defence System Institute
    Singapore

13. Chang Xuquan Stanley
    Student, Naval Postgraduate School
    Monterey, California

14. Chua Kim Yong
    Student, Naval Postgraduate School
    Monterey, California