CyberCIEGE: An Extensible Tool for Information Assurance Education

Cynthia E. Irvine, Senior *Member, IEEE*, Michael F. Thompson, and Ken Allen

Abstract – The purpose of CyberCIEGE is to create an extensible Information Assurance (IA) teaching and learning laboratory. Through a scenario definition language, educators can create simulations to demonstrate specific IA concepts. In addition to rigorous scientific foundations, it involves the application of abstract principles to a virtual world. This hands-on virtual laboratory provides a dynamic and often surprising context where abstract principles can be applied.

Index terms – Information Assurance, Education, Simulation, Virtual World

I. Introduction

The concept of using games to support health, education, management, and other sectors has resulted in a high level of interest and activity [1]. The tacit knowledge gained by applying concepts in a virtual environment can significantly enhance student understanding.

A number of games have been developed involving protection of assets in cyberspace. Some teach information assurance concepts, e.g. CyberProtect [2], while others provide pure entertainment with no basis in information assurance principles or reality [3]. None have presented an engaging virtual world that combines the human and technical factors associated with an IT environment. In addition, these games are limited in the scope of information assurance topics covered. Short of going back to the creator for a new version, there is no way add new material to the game.

* *Naval Postgraduate School, Monterey, CA.* irvine{Thompson}@nps.edu
** *Rivermind, Inc.* kallen@rivermind.com
Development of CyberCIEGE was sponsored by the U.S. Navy, the Naval Education and Training Command, the Office of Naval Research, and the Office of the Secretary of Defense. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.
CyberCIEGE is a Trademark of Rivermind, Inc.

To address this problem and to create a tool applicable in teaching contexts ranging from introductory training and awareness to the sophisticated concepts of graduate-level courses, we embarked on a project to create an information assurance video game. The result is CyberCIEGE, a video game that packages an information assurance laboratory as an interactive, entertaining, PC-based computer game. In each scenario, players assume the role of the IT manager who must keep the IT infrastructure running in support of various enterprise goals, while making technical and administrative choices regarding the security of that infrastructure. The consequences of these choices are reflected in the success of either the enterprise or of external adversaries.

This paper describes the motivation for CyberCIEGE and the basics of resource management games. Essential components of CyberCIEGE are presented along with an overview of typical game play. How CyberCIEGE can be used by educators to enhance information assurance classes as well as a description of the "open source" paradigm available for sharing CyberCIEGE scenarios and related teaching materials will be discussed.

II. Motivation

Information assurance education covers an enormous range of topics. Introductory classes can barely touch on each topic much less provide in-depth presentations of complex issues. Thus, mature information assurance programs contain both introductory and advanced classes, as Table 1 illustrates for our university. Courses are categorized by type: introductory or advanced. Laboratories are required for all of the courses as they are considered essential for conveying complex concepts [4]. Often, hands-on laboratory experience helps students understand how access control lists, mandatory security or even Trojan Horses work.

A significant challenge to educators attempting to develop information assurance curricula is the dynamic nature of the topic. The time and resources required to develop and

maintain IA courses is often formidable and laboratory exercises may lag behind the development of lectures.

Class Name	Type	Lecture/Lab Hrs.
Introduction to Information Assurance	Intro	4/2
Critical Infrastructure Protection	Intro	3/1
Secure Management of Systems	Intro	3/2
Network Vulnerability Assessment	Intro	3/2
Network Security	Adv	4/1
Secure Systems	Adv	3/2
Database Security	Adv	3/1
Security Policies, Models and Formal Methods	Adv	3/1
Computer Forensics	Adv	3/2
Information Ethics and Law	Adv	3/2
Introduction to Certification and Accreditation	Adv	3/2
Advanced Topics in Computer Security	Adv	3/1

Table 1. Sample Mature IA Curriculum

Another problem facing many educators is high student demand combined with a lack of resources. Information Assurance courses can quickly attract a large number of students and it often takes years to build the infrastructure required to support extensive laboratory exercises.

Too often, education can be boring. Also, effective education requires a tacit understanding of the art of security engineering. Thus IA education can benefit from an engaging and sometimes surprising presentation that captures the user's imagination. Interactive simulations show promise as educational tools. By generating a sense of competition, these tools, often in game-like formats, provide an exciting environment in which the participant has a stake in the outcome. For many learners, visualization, associated with kinetic activity, helps to teach or re-enforce concepts. CyberCIEGE [5] [6] has been designed to address many of these problems.

III. A Resource Management Simulation

The potential for resource simulation tools to capture a user's attention is illustrated by the success of games such as SimCity™ and RollerCoaster Tycoon®. In these games, players engage in planning and construction and observe the results of their choices. The many hours devoted to these games and the deep knowledge of the games exhibited by the players indicate an experiential and process reflecting both an emotional and an intellectual investment. CyberCIEGE has a similar goal.

The player assumes the role of a decision maker for an IT-dependent organization. The objective is to keep the organization's virtual users happy and productive while providing the security measures needed to protect valuable organizational information assets. Within a given CyberCIEGE scenario, the player has a budget and must make choices regarding procedural, technical and physical security. With good choices the organization prospers and the scenario advances; poor choices often result in disaster. CyberCIEGE uses the potential tension between strong security and user productivity to illustrate that many security choices are an exercise in risk management.

The student is immersed in an environment where his or her choices have visible effects on the ability of virtual users to perform productive work and on the ability of attackers to compromise assets. Students build and configure networks of computers. The scenarios strive to give the user an emotional attachment to that which they have built, thereby providing a more acute learning experience when bad decisions lead to loss.

The tool includes several different scenarios, each of which is run separately. Each scenario includes a briefing that describes an enterprise (e.g., a business that manufactures bowling balls) and gives the player information about what must be done to help make the enterprise successful. Within each scenario, the enterprise has a defined set of users and assets. Users are typically employees of the enterprise whose productive work makes money for the enterprise. Assets are various kinds of information that users must access to be productive. Examples of assets are secret formulas, corporate accounting information, business plans, expense statements, and marketing material. Each enterprise has a number of different virtual users who each need to access different assets in different ways to be productive for the enterprise. These are *user goals*. And sometimes, assets need to be shared among users, who may also need to simultaneously access multiple different assets. Different assets have different secrecy, integrity and availability values, and different users have different authorizations to access assets as defined by the enterprise security policy.

Artwork, as shown in Figure 1, enhances the ambiance of each scenario.

Each scenario is characterized by predefined users, assets, user goals and an enterprise security policy. Once established, they are not subject to change by the student. What distinguishes CyberCIEGE is the limitless number of possible scenarios that can be created to teach IA.

Figure 1: CyberCIEGE user at work

IV. CyberCIEGE Components

CyberCIEGE consists of several elements: a unique simulation engine, a scenario definition language, a scenario development tool, student assessment logs and a video-enhanced encyclopedia. CyberCIEGE is extensible in that new scenarios tailored to specific audiences and topics are easily created. Scenario-based event triggers are used to introduce new problems to be solved and to generate log entries for subsequent student assessment.

A major objective in the development of CyberCIEGE was to create a tool for which a large number of scenarios could be developed. This was motivated by two factors. First, information assurance involves an huge number of topics. We concluded that many scenarios with different points of focus and depth of detail are needed to begin to cover the large number of IA topics. Some scenarios are lengthy, while others are short and focus on specific security concepts. This allows IA educators to tailor scenarios for particular teaching objectives.

The second factor driving the creation of an extensible tool is to allow advanced students to create their own scenarios. Here, a student must create an information security policy from whole cloth and imagine the tensions that could develop from trying to enforce the policy while letting users achieve their goals. This provides the potential for students to encounter scenarios that cannot be won, e.g., due to unenforceable information security policies.

A. Simulation Engine

At its foundation, CyberCIEGE contains a sophisticated simulation engine, the Rivermind-proprietary TYBOLT game engine, a next generation console-based engine

designed for both games and simulations. At its heart is a multi-platform 3D graphics library that supports imported, standards-based objects and animations as well as Windows-like user interfaces within a fully 3D environment. The engine contains an artificial intelligence system, a video playback library, a sound library, a memory management system, a resource management system, and a real-time strategic, network and economic engine.

Several scenarios were created to test the simulation engine during its development [7][8][9][10].

B. Scenario Definition Language

CyberCIEGE is built around a language that expresses security-related risk management tradeoffs for different scenarios. The CyberCIEGE simulation engine interprets this scenario definition language and presents the student with the resulting simulation. The scenario as expressed using the scenario definition language defines the student experiences and the consequences of the player choices. The language includes the following major elements:

Assets: Information of some value to the enterprise. The virtual users access assets as part of achieving their asset goals. Examples of assets are secret formulas, corporate accounting information, business plans, expense statements, and marketing material. Some assets are of high value to the enterprise, while others are inconsequential. Thus there is a *cost* to the enterprise if the asset is compromised. Assets have different *motive values* to attackers, resulting in different levels of motivation for attacks against the assets. Some assets have value to attackers because they are secret (e.g., proprietary manufacturing data). Other assets have value because of their integrity (e.g., authoritative accounting records). Some assets have security labels, and the value of labeled assets is separately described. Thus a variety of assets can have a "Proprietary" label, and each asset with that label inherits the same cost and motive values. A given asset can have cost and motive values derived from a label as well as values explicitly tied to other users, i.e., to express discretionary security policies.

Users: Each CyberCiege scenario includes a set of virtual users whose productive work makes money for the enterprise. Users have work goals that must be met for the users to remain productive and happy. The student is responsible for providing the resources and environment needed by users to reach their goals. Each user has one or more goals expressed as a need to access specific assets. Some goals can express a rather abstract desire such as: "Joe wants to receive email from the Internet." Other goals express more detail such as: "Mary wants to use the Data Inversion Application software program to modify the secret sauce asset while reading the production schedule asset." Some user goals are correlated with that user's productivity. Other goals relate to a user's happiness (e.g., a desire to surf the Internet or get personal email). If a user fails to achieve productivity goals, it can directly affect the enterprise's bottom line. Failing to achieve a happiness goal does not directly affect the bottom line, but may eventually result in a disgruntled employee, which can ultimately impact enterprise security.

Zones: Each scenario includes one or more physical zones that can be used to control the physical movement of users. An example of a zone is a physically secure office with a locked door for which only selected users have a key. When IT components are purchased, they are placed within a specific zone. Physical access to components can therefore be constrained based on the physical access to the zone. As shown in Figure 2, the entire office is itself a zone, and it can contain additional zones to which additional security measures are applied.

Conditions and Triggers: The scenario designer defines conditions to be assessed by the engine during play, and

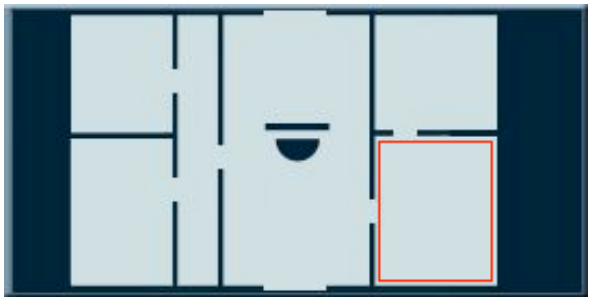

Figure 2: Office floor plan highlighting a zone

specifies actions to occur as the result of a combination of conditions. For example, at some point in the simulation, a virtual user can receive a new asset goal, requiring the player to take actions to enable the user to achieve the goal. Or the scenario designer can cause specific types of attacks to occur (or not occur) depending on different conditions such as elapsed time and whether users are achieving goals. Player progress, hints and complaints from unhappy users can appear using pop-up windows and a moving message ticker at the bottom of the screen. Winning and losing are also defined using conditions and triggers. This allows the scenario designer to present the student with different debriefing screens dependent on the reason the game was lost.

Objectives and Phases: Scenarios can be divided into several phases, each consisting of one or more objectives. Objectives are defined in terms of conditions, as described above. The student must achieve each objective in a given phase before the simulation will transition to

the next phase. This permits the scenario designer to guide the student through the scenario and gives the student an incremental sense of achievement.

C. Scenario Development Tool

The Scenario Definition Language (SDL) allows educators to construct their own scenarios, or extend and enhance existing scenarios. The language is quite rich and syntactically intensive. Construction and maintenance of SDL text files by hand can be a substantial challenge requiring several thousand lines of text to express a full scenario. A forms-based Scenario Development Tool (SDT) was created to ease the process of expressing a scenario in the language [11]. Using the SDT, the scenario developer does not have to understand the SDL syntax to construct and modify scenarios. Furthermore, the SDT enables scenario designers to construct scenarios from a library of re-usable scenario elements. The library consists of "scenario element sets", each of which contains one or more SDL elements. For example, a scenario element set can contain one or more assets, or one or more users. Scenarios are constructed by pulling together various scenario element sets.

As shown in Figure 3, the SDT displays a graphical representation of the scenario. The lower left pane represents all scenario element sets within the current scenario. The upper left pane is the library of sets that could be included within the scenario. A tabbed work area displays selected scenario element sets as individual tabs, and the currently selected element of the set as a form.

Each major element of the SDL is represented in its own SDT form. Figure 3 includes the form that defines an asset. Pull-down lists are automatically populated with applicable items that are defined as part of the scenario under development. For example, when constructing an access control list for the asset, the user selects from user names that have been defined as part of the scenario.

CyberCIEGE has been designed so that a single scenario can be a well-defined information assurance teaching unit. Using the concept of a *campaign*, these teaching units may be combined to create a coherent succession of scenarios that provides either a succession of progressively more difficult scenarios or a focused educational unit that covers several topics [12].

Multiple scenarios within a campaign can easily share scenario element sets from the library. The developer simply adds the sets to each scenario. This ability to share and reuse libraries simplifies the construction of sequences of scenarios intended to illustrate information assurance concepts through contrasting policies. For example, the scenario designer can construct two nearly identical scenarios whose only difference is the attacker motive to compromise a given asset.

Reusable libraries also ease the testing of scenarios by letting the designer construct test jigs that can be quickly inserted and removed from scenarios to simulate possible player actions. Imagine that the scenario designer wishes to test the effects of a player choice to buy several computers and configure them in different ways. Instead of playing the game, making the purchases and manually configuring the components, the designer can define the components within a scenario element set that is added to the scenario only when the designer wishes to perform that test.

The SDT is integrated with the CyberCIEGE game itself. The menu allows the developer to launch the game using the scenario currently under development. The menu also provides the developer with easy access to logs created by the game for testing and debugging of scenarios. Additionally, the SDT is capable of importing games that were saved by the player. The developer can therefore use the game itself to construct a network topology and import the results into the SDT.

D. Student Assessment

The CyberCIEGE engine generates a log of player choices and game events (e.g., the compromise of assets). At the end of a scenario, the player can view a summary of the log as a debriefing. The log is also intended to allow educators to assess student success in each scenario. The trigger subsystem (described earlier) lets the scenario designer generate custom log entries depending on specific game conditions. The scenario designer can anticipate common player mistakes for a given scenario and generate log entries that are specific to both the mistake and the scenario. For example, a scenario illustrating virus controls could produce a highlighted log message if the player takes a network operational without instructing virtual users to not open executable attachments. This saves the instructor from having to parse the log for entries on individual configuration decisions. Through the use of log triggers, the scenario designer can enhance the educator's ability to assess student comprehension and progress.

E. Encyclopedia

To complement the interactive virtual environment, CyberCIEGE contains an encyclopedia. At any time during a scenario a student can invoke the encyclopedia. Here the student is presented with a menu leading to a variety of topics. Some encyclopedia entries teach the student how to play the game. They include a description of the constants within scenarios and the elements of the

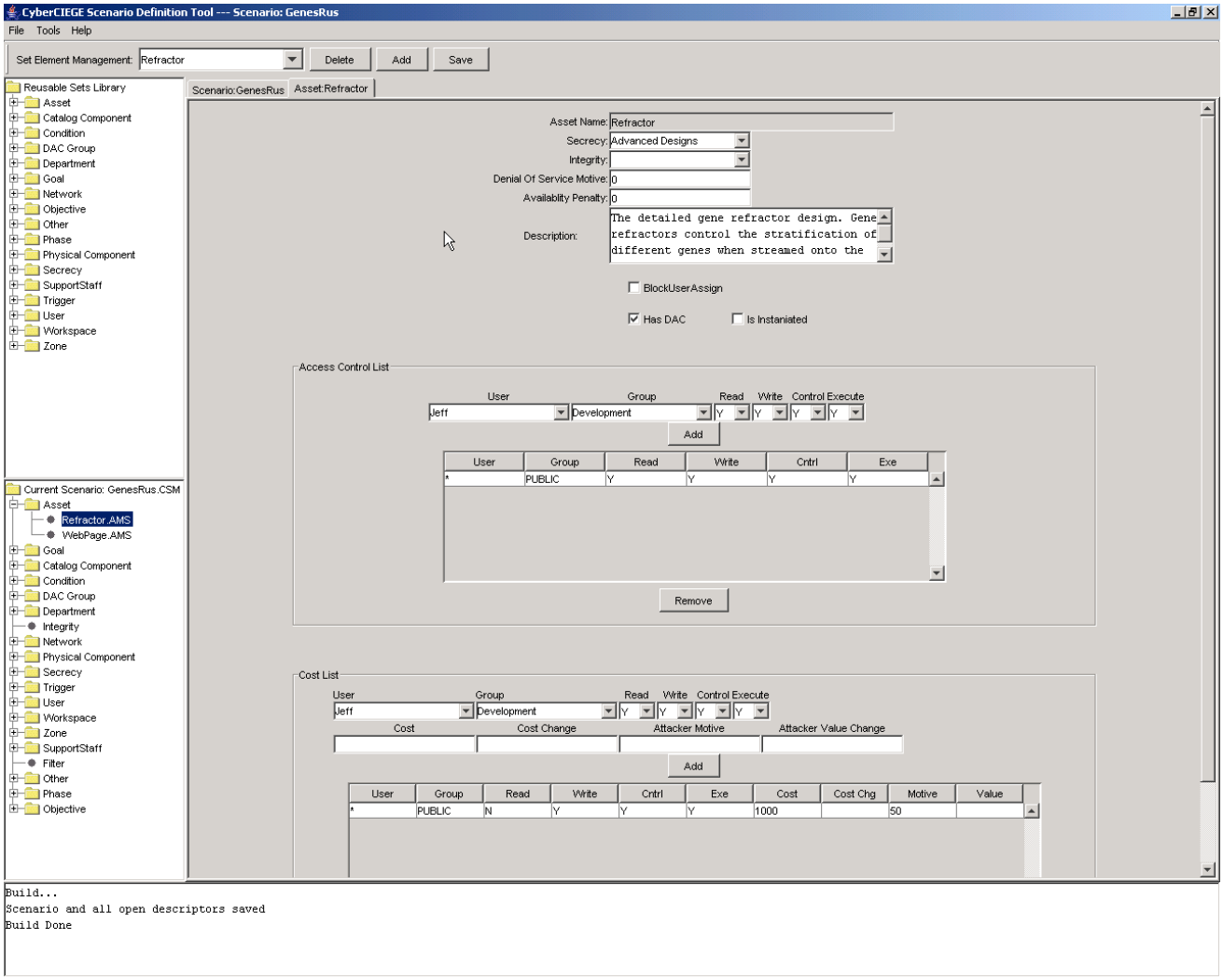

Figure 3: Scenario Development Tool

scenario over which the user has control. Students can learn how to tell if they are winning or losing.

A set of encyclopedia entries describes a broad range of information assurance topics. These include descriptions of policy, passwords, network security devices, malicious software, access control mechanisms, etc.

Movies complement material in the encyclopedia. They are designed to be entertaining to all age groups. The initial release contains movies about security policy, malicious software, firewalls, and assurance, as well as a movie describing how to use CyberCIEGE.

V. Student Interface to CyberCIEGE

Scenarios start with a briefing that describes the scenario and the enterprise for which computer resources must be managed. Player responsibilities may include configuring and networking existing computer components; making physical security and procedural security choices; and hiring information technology support staff. Sometimes the student must purchase specific computer components and connect them to networks.

With a limited budget, the player must make money for the enterprise by efficiently and securely managing the enterprise computer networks. Each virtual user's needs to access different assets, i.e., the user goals, must be understood. The users must have suitable computer components, software, network interconnections and technical support personnel to achieve their goals of accessing assets.

An environment where the assets are protected in accordance with the enterprise security policy must be created and maintained. Failure to adequately protect the assets results in monetary losses to the enterprise due to

direct loss, and lost user productivity. Several kinds of choices affect the protection of assets in accordance with the security policy:

- Selection and deployment of components in topologies suitable for security policy enforcement.
- Component configuration.
- Interconnect components using networks.
- User instruction and training.
- Physical security restrictions.
- User background check levels.

These security choices affect the protections provided to the enterprise assets, which are subject to attack from vandals, disgruntled employees, professional attackers, incompetent users and acts of nature.

Students can start and pause the simulation at any time. Typically, players are encouraged to construct networks and make policy enforcement decisions prior to starting the simulation. This is analogous to configuring and assessing a deployed system prior to taking it operational. After the student starts the simulation, virtual users may start creating and accessing their assets, and without due care, this may occur in ways that make the assets vulnerable to attack.

During the game, players can select and observe the status of a user's productivity and happiness. Users unable to achieve their goals become visibly agitated. A message ticker at the bottom of the screen and pop-up messages can inform players of their progress.

VI. Benefits and Application of CyberCIEGE

CyberCIEGE affords educators a number of advantages. As a virtual laboratory, CyberCIEGE does not require an extensive infrastructure. For example, students can experiment with costly high assurance components in the game's virtual world and the college or university does not have to incur the cost of such a system. The heterogeneous mixture of component types and assurance levels available in the game provides an opportunity for students to gain experience with a wide range of topologies and systems.

The first commercial version of CyberCIEGE was released by Rivermind Inc. (www.rivermind.com) in April 2005. Before then, several colleges and universities had acquired demonstration copies. In this section, we present some ideas for CyberCIEGE use in the classroom.

CyberCIEGE is not what is commonly known in the industry as a "twitch game". However engaging and entertaining, it is not a game where the player constantly presses buttons to avoid pending disasters as a hypothetical game "Suring at Mavericks" might. Hence, educators may not want to merely hand CyberCIEGE to students and tell them to "have fun." Scenarios force students to stop and think about what they are doing.

Educators can tailor the game to their teaching objectives. The Scenario Definition Language, when combined with the Scenario Definition Tool allows educators to create either simple or sophisticated scenarios. Each scenario is designed to tell a story. The interplay between asset values, virtual user goals, and attacker motivation drives the story. Triggers can introduce new factors into the game. The use of phases can tell the story in chapters.

The richness of the SDL and simulation engine allow very complex topics to be presented. It is possible for educators to develop scenarios for which there is no effective solution, thus challenging the creativity of advanced students to explore new research areas.

Just as games intended for pure entertainment benefit from user communities and forums, games focused on education can benefit from sharing by a community of users. For CyberCIEGE, the community consists of new and experienced information assurance educators.

A CyberCIEGE website has been created http://cisr.nps.navy.mil/cyberciege.html. The site contains information about the tool and provides contact information, such as the CyberCIEGE email address: cyberciege@nps.edu. Updates to the game, a description of the SDL, the SDT, encyclopedia, movies, etc. are all available for download from the website. Most importantly, scenarios are available at the website.

Using an "open source" paradigm, the web site is intended to provide a location where educators can submit and share scenarios with others. New scenarios will be reviewed prior to posting on the web site to ensure appropriateness and quality control. For example, one educator might add a relatively simple scenario about routers. A second educator could modify or add to that scenario perhaps by making the network configurations more complex. A third educator might extend the scenario further by establishing a more granular organizational policy. In this way a suite of scenarios would be available for others to download and use.

VII. Summary and Future Work

CyberCIEGE is an innovative computer-based tool that can augment an information assurance education program. Its extensibility will allow educators to develop scenarios tailored to their classes, while the open sharing model will allow educators to share and reuse scenarios. The engaging nature of the game can capture the

imagination of students and illuminate concepts that are difficult to convey through lectures alone.

A. Enhancements to the Current Tool

Clearly, additional scenarios will enhance the game for a broad range of educators.

NPS and Rivermind anticipate partner agencies interested in tailoring the tool to meet their specific IA teaching requirements. In some cases this may involve improvements to the simulation engine and its attendant tools. Both Rivermind and NPS seek feedback on CyberCIEGE, which can be provided via feedback and bug report interfaces at the game website.

An assessment tool is planned that will allow educators to more easily visualize how well students are learning the material presented in the game. For large organizations involved in training or teaching hundreds or even thousands of students, a grading tool would be of value.

Human factors is another area of CyberCIEGE research. The effectiveness of the game in teaching various age groups and genders could be examined. The impact of the game itself and of sound and visual cues on student understanding and knowledge retention should be studied. Materials and presentations to help educators start creating scenarios and using CyberCIEGE effectively can be developed. These may include tutorials or workshops.

B. Advanced CyberCIEGE Versions

Possible advanced versions of CyberCIEGE include: a wireless version and a multiplayer version.

1. Wireless Security Version

The current version of CyberCIEGE contains no mobile, wireless components. The overlay of such technology on the existing simulation would result in a significant advance in the ability of the tool to depict emerging network-centric architectures. New scenarios involving traveling users would further extend IA education.

2. Multiplayer Version

A multiplayer version of CyberCIEGE would allow students to protect and provide computer services to their virtual organizations challenging the information assurance measures of their competitors. This will require major changes to the scenario definition language as well as to the underlying simulation engine. The resulting game would present IA topics in a highly dynamic, competitive environment. Preliminary studies for a multiplayer version are currently underway.

REFERENCES

[1] Serious Games, http://ww.seriousgames.org/ Last Accessed: 3 March 2005.

[2] CyberProtect, http://iase.disa.mil/eta/index.html Last Accessed: 28 February 2005.

[3] Nexus Interactive. “AI Wars: The Awakening”. http://www.aiwars.com/ Last Accessed: 27 January 2005.

[4] Irvine, C. E., “Amplifying Security Education in the Laboratory,” Proceedings of the First World Conference on Information Systems Security Education, Stockholm, Sweden, pp. 139-146, June 1999.

[5] Irvine, C. E., and Thompson, M., “Teaching Objectives of a Simulation Game for Computer Security,” Proceedings of Informing Science and Information Technology Joint Conference, Pori, Finland, June 2003.

[6] Irvine, C. E., and Thompson, M., “Expressing An Information Security Policy Within A Security Simulation Game,” Sixth Workshop on Education in Computer Security, Monterey CA, July 2004. http://cisr.nps.navy.mil/downloads/WECS6_Proceedings.pdf LastAccessed: 27 January 2005

[7] Fielk, Klaus W., CyberCIEGE Scenario Illustrating Integrity Risks to a Military-Like Facility, Masters Thesis, Naval Postgraduate School, Monterey, CA, September 2004.

[8] Lamorie, J. A CyberCIEGE Scenario Illustrating Secrecy Issues in an Internal Corporate Network Connected to the Internet, Masters Thesis, Naval Postgraduate School, Monterey, CA, Sept. 2004.

[9] LaMore, R. L., CyberCIEGE Scenario Illustrating Secrecy Issues Through Mandatory and Discretionary Access Control Policies in a Multilevel Security Network, Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[10] Meyer, M. K., A CyberCIEGE Scenario Illustrating Multilevel Secrecy Issues in an Air Operations Environment, Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[11] Johns, K. W. Toward Managing and Automating CyberCIEGE Scenario Definition File Creation,” Masters Thesis, Naval Postgraduate School, Monterey, CA, June 2004.

[12] Teo, T. L., Scenario Selection and Student Selection Modules for CyberCIEGE, Masters Thesis, Naval Postgraduate School, Monterey, CA, December 2003.