available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A video game for cyber security training and awareness

Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, Thuy D. Nguyen*

Department of Computer Science, Center for Information Systems Security Studies and Research, Code CS/Ic, Naval Postgraduate School, Monterey, CA 93943, USA

Keywords:
Information assurance
Training and awareness
Educational simulation
Video game
Network security

ABSTRACT

Although many of the concepts included in cyber security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organization. In addition, many forms of training fail because they are rote and do not require users to think about and apply security concepts. A flexible, highly interactive video game, CyberCIEGE, is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure. The game is now being successfully utilized for information assurance education and training by a variety of organizations. Preliminary results indicate the game can also be an effective addition to basic information awareness training programs for general computer users (e.g., annual awareness training.)

1. Introduction

Typical employees of both large and small organizations may be made acutely aware of a wide array of cyber security problems. These range from spam and phishing to well organized attacks intended to corrupt or disable systems. Despite these constant reminders, users often take an ostrich-like attitude toward the security of the information systems they use, believing that there is little that they can do to mitigate this onslaught of problems. Even within the major organizations, users select trivial passwords or think that, so long as they keep their machines within viewing distance, arbitrary hookups to unknown networks and to the Internet pose no threat. Thus, despite their increased awareness of security problems, users and administrators of systems continue to take few effective precautions. Yet, to achieve an adequate security posture, organizations must combat this user apathy with effective training and awareness programs. The enormity of the problem associated with effective user training and awareness is evident in that it was considered one of five areas of highest priority for action in a national plan for cyberspace security (EOP, 2003).

Human factor studies illustrating the need for user training and awareness are well documented, e.g. (Whalen, 2001). The concept of using games to support health, education, management, and other sectors has resulted in a high level of interest and activity (Prenski, 2001). 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 (DoD, 1999), whereas others provide pure entertainment with no basis in information assurance principles or reality (Nexus, 2003). 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

* *Corresponding author.*
E-mail addresses: benjamin.cone@hotmail.com (B.D. Cone), irvine@nps.edu (C.E. Irvine), mfthomps@nps.edu (M.F. Thompson), tdnguyen@nps.edu (T.D. Nguyen).
0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.10.005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A video game for cyber security training and awareness	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School ,Center for Information Systems Security Studies and Research (NPS CISR),Department of Computer Science,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Although many of the concepts included in cyber security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organization. In addition, many forms of training fail because they are rote and do not require users to think about and apply security concepts. A flexible, highly interactive video game, CyberCIEGE, is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure. The game is now being successfully utilized for information assurance education and training by a variety of organizations. Preliminary results indicate the game can also be an effective addition to basic information awareness training programs for general computer users (e.g., annual awareness training.)

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**10**	

a new version, there is no way to add new material to the game.

Effective user security awareness training can greatly enhance the information assurance posture of an organization (NIST, 1993). Yet holding a trainee's attention sufficiently long to impart a message is a considerable challenge, particularly when the training is mandated and the target audience views the topic as potentially mundane. Video games have been proposed as an engaging training vehicle (Prenski, 2001). Here we describe a video game-like tool called CyberCIEGE and how it was employed to develop security awareness training targeted for the requirements of a specific organization, and how this extensible tool can offer training and education for a range of target audiences. For this analysis, training for uniformed and civilian personnel associated with the U.S. Navy has been conducted.

CyberCIEGE is unique in that it is a highly extensible game for teaching information assurance concepts. It may be applied to a wide range of audiences having different levels of technical sophistication. It has its own language for creating new educational scenarios and is accompanied by tools and tutorials that help instructors develop customized scenarios.

We start with a review of commonly used training and awareness techniques, and follow with an overview of CyberCIEGE and a more detailed description of how scenarios for the game are constructed. At this point, it will be possible to examine policies for information assurance training and awareness of our target organization and then describe a targeted requirement analysis. How two CyberCIEGE scenarios, one for general awareness and the other for IT personnel, were created to fulfill organizational information assurance training and awareness requirements will follow. This work concludes by pointing to several new directions for further development of the CyberCIEGE educational tool.

2. Background

To provide a context for subsequent discussion of CyberCIEGE as a tool for user training and awareness in information assurance, it is useful to review both current training and awareness methods as well as provide an overview of CyberCIEGE.

2.1. *Common current training and awareness techniques*

Training and awareness is generally accomplished using one or a combination of several techniques described below.

Formal Training Sessions can be instructor-led, brown-bag seminars, or video sessions. Formal training in sessions facilitated by local information security personnel represents the traditional approach to user training and awareness within the Department of the Navy. The success of this approach depends upon the ability of the training facilitator to engage the audience.

Passive computer-based and web-based training represents a centralized approach to the training and awareness problem. An example is the web-based training in information assurance offered by the U.S. Department of Defense (DoD, 2006). CBT offers the user the flexibility of self-paced training, and provides the organization with the ability to train users to an enterprise-wide standard. Its disadvantage is that training and awareness becomes a monotonous slide show that fails to challenge the user and provides no dialogue for further elaboration. Often, users attempt to complete CBT sessions with minimal time or thought. The CBT developer must attempt to provide engaging instruction within the constraints of a passive medium.

Strategic placement of awareness messages seeks to raise the level of consciousness through the delivery of messages in the workplace. Some of the more common delivery methods include organizational newsletters and memos, email messages, posters, screen savers, and security labels, e.g. posters highlighting various cyber security risks (CCS, 2006).

Interactive computer-based training, such as a video game, generally falls into two broad classes: first-person interaction games or resource management simulations. The majority of games falls into the first category and include first-person shooter games where the player is confronted by an adversary or problem and must take an appropriate action or is penalized, sometimes severely. In contrast, resource management games require the player to manage a virtual environment using limited resources. The player attempts to make choices that improve the environment within the constraints of the available resources. Good choices result in a richer environment and additional resources. SimCity™, other "sims" games, and RollerCoaster Tycoon (R) are popular examples of resource management games.

Games and simulations have become increasingly accepted as having enormous potential as powerful teaching tools that may result in an "instructional revolution" (Foreman, 2004). Prenski (2001) and Gee (2005) have provided a framework to construct and analyze games in education. The latter has described the context of a specific game as a semiotic domain that allows students to learn an area through use and experience while leading the student to approach problem solving through critical thinking. Analysis of the effectiveness of games is in its infancy; however, pioneering work (Gee, 2003; Aguilera and Mendiz, 2003; Squire, 2005; Gredler, 2004) is beginning to show that games offer an effective alternative to, or supplement for, more traditional modes of education. For example, through the use of virtual worlds, games provide a concrete experience within which students can internalize domain-specific concepts. Student's critical thinking skills are honed. In addition, the game format often appeals to students with short attention spans.

2.2. *CyberCIEGE*

In 2005, the Naval Postgraduate School released an U.S. Government version of CyberCIEGE, a video game intended to support education and training in computer and network security. Simultaneously, our collaborators at Rivermind, Inc. made a version available to non-government organizations. The game employs resource management and simulation to illustrate information assurance concepts for education and training (Irvine and Thompson, 2003, 2004). In the CyberCIEGE virtual world, players construct and configure the computer networks necessary to allow virtual users to be productive and achieve goals to further the success of the enterprise. Players operate and defend their networks, and can

watch the consequences of their choices, while under attack by hackers, vandals and potentially well-motivated professionals.

2.2.1. *CyberCIEGE components*

The building blocks of CyberCIEGE consist of several elements: a unique simulation engine, a domain-specific scenario definition language, a scenario development tool, and a video-enhanced encyclopedia (Irvine et al., March 2005). CyberCIEGE is intended to be extensible in that new CyberCIEGE scenarios tailored to specific audiences and topics are easily created (Irvine et al., June 2005).

The scenario definition language expresses security-related risk management trade-offs for different scenarios. The CyberCIEGE simulation engine interprets this scenario definition language and presents the player with the resulting simulation. What the player experiences and the consequences of the player choices are a function of the scenario as expressed using the scenario definition language.

The game engine and the language that feeds it are rich in information assurance concepts so that it is possible to simulate sophisticated environments subject to a variety of threats and vulnerabilities. They also include substantial support for relatively brief, scripted training and awareness scenarios. This support includes cartoon-like balloon speech by the virtual users, message tickers, pop-up quizzes and conditional play of video sequences, e.g., a computer worm.

So that educators are able to assess their students, CyberCIEGE also produces a log of player activity. Triggers within the scenario cause output to be appended to the log where a number of status indicators may be recorded. A separate log is maintained for each player, thus allowing the instructor to track the progress of individual students.

The set of CyberCIEGE components is illustrated in Fig. 1.

2.2.2. *Development and Testing of CyberCIEGE*

The collaborative development of CyberCIEGE was an iterative process by video game developers with little knowledge of information assurance, and information assurance technologists with little background in video games. Early focus was on establishing a language that would allow us to construct scenarios as per our broad teaching objectives (Irvine and Thompson, 2003). This scenario development language evolved around a core ability to express a security policy in terms of users and information (Irvine and Thompson, 2004). The game developers built the CyberCIEGE game engine using C++ and their 3D graphics library. The engine was designed to consume the scenario definition language and behave in a logically consistent manner.

Some scenario language elements were relatively straightforward to represent in the game engine. For example, the costs of purchasing computer equipment, or the penalties incurred when users were not able to achieve goals are conceptually straightforward, and have analogues in other resource management games. Innovation was required to automate assessment of vulnerabilities in networks constructed by players such that the game could mount credible attacks. The attack logic within the game engine required several iterations and considerable testing. Dozens of test scenarios were generated to exercise the engine's response to a range of topologies, component configurations and attacker motives. Ultimately, some of the attack logic within the game engine was built around the tests rather than to any precise specification. For most scenarios, this has proven adequate. The resulting attack engine represents a range of security policies, including those modeled by Bell and LaPadula (1975) and Biba (1977), as well as discretionary security policies (Lunt, 1989; Bishop, 2002).

CyberCEIGE has been the basis for several master theses at NPS in which students developed their own scenarios. This

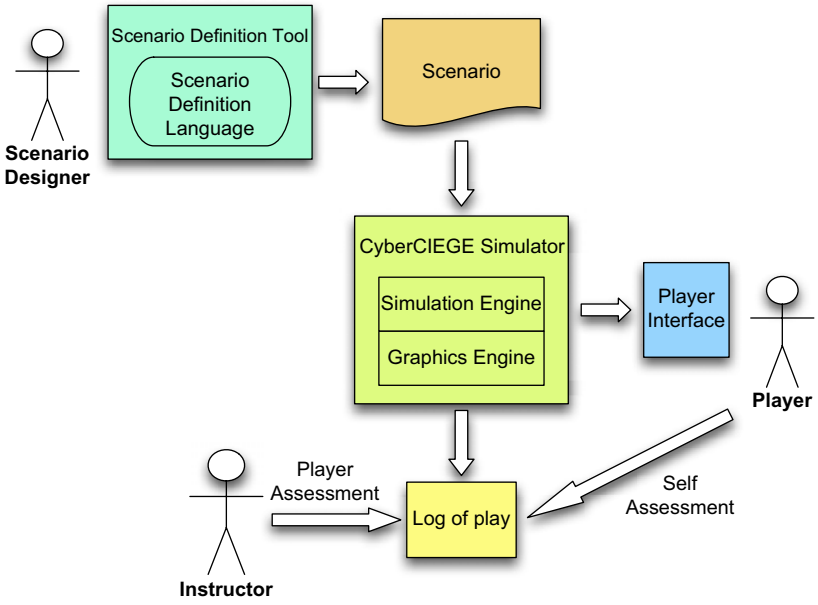

Fig. 1 – CyberCIEGE components.

early exercising of the CyberCIEGE engine provided considerable breadth and depth of informal testing. The CyberCIEGE user interface has undergone more formal testing by the Pacific Northwest National Laboratories (Roberts et al., 2006). That testing resulted in several refinements of the game interface.

The scenario development tool (Johns, 2004) and the related tools (Teo, 2003) were developed using Java. And again, student theses work provided substantial informal testing of these tools.

The game and the tools all are designed to run on the Windows 2000 and Windows XP operating system. The graphic libraries make considerable use of the DirectX interface to render the three dimensional world.

3. Scenario construction

Story telling is the key to a good CyberCIEGE scenario. The player should readily grasp the nature of the virtual environment (e.g., a small business with valuable intellectual property) and the types of choices that he has to make. Within this context, the player should have reason to care about the ramifications of these choices.

Scenario designers utilize the scenario definition language to construct a virtual environment that drives players to make resource management decisions. These player choices affect the productivity of an enterprise, and affect the vulnerability of information assets to compromise by virtual attackers. The CyberCIEGE game engine interprets the scenario definition language, presenting the player with a virtual environment as defined by the designer. To construct a scenario, the designer must understand the semantics of the scenario definition language and the capabilities of the CyberCIEGE game engine. A form-based integrated development environment allows designers to construct scenarios without mastering the syntax of the design language (Johns, 2004).

3.1. *Programming the CyberCIEGE game engine*

In every CyberCIEGE scenario, the player is the information assurance decision maker for some enterprise. An enterprise may be a large military facility, or it may be a home office. The fundamental abstractions within the CyberCIEGE game engine are not computers, networks and protection mechanisms. Rather, they are assets, users, and attackers (Irvine and Thompson, 2003). Assets are information resources. Users are typically employees of the enterprise who have goals that require computerized access to assets. Players succeed by facilitating user access to assets. Some assets have substantial value to the enterprise based on secrecy or integrity. And some assets may have value based on their availability. Assets also have value to attackers, and this motive determines the means by which the attacker will attempt to compromise an asset. Player choices affect the opportunity (or lack thereof) for the attacker to compromise the assets. The enterprise (and by extension the player) is penalized the value of an asset should it be compromised or made unavailable.

Within any given scenario, the users, assets, and attackers are for the most part fixed by the designer and are not modified by player choices. Designers also specify the initial state of the scenario (e.g., an initial set of computers) and dynamic changes to the scenario (e.g., the introduction of new user goals.)

Players see the enterprise as an animated three dimensional representation of an office building or military headquarters. Each scenario has one main office and an optional small offsite office. Users inhabit these buildings, wandering about or productively sitting at desks in front of computers. If computers are available, either as a scenario default or through purchase by the player, users will create and access assets using the computers. This user behavior is driven by the user goals specified by the designer. If computers are networked together, users may access assets over the network. Network devices such as routers enable users to access the Internet, and allow attackers on the Internet to potentially access enterprise resources. Suitably motivated attackers can enter buildings to compromise assets. They may compromise computer-based protection mechanisms, and may wiretap network links. Attackers may also bribe untrustworthy users to compromise assets. Finally, users themselves may have motive to compromise assets.

Players may hire guards to help with the physical protection of buildings or offices within buildings. Players may purchase physical protection mechanisms such as alarms and they may select which users are permitted to access different physical areas (i.e., ''zones'') within the virtual buildings. Procedural security choices affect user behavior (e.g., leaving computers logged in). Players can purchase user training to improve user adherence to procedural policies.

3.2. *The game engine as illustrated with a simple scenario*

Consider a scenario consisting of a single asset and a single user having a goal to read the asset. If this scenario is fed to the CyberCIEGE engine, the user will fail to achieve the goal of reading the asset until the player buys the user a computer. The designer associates a productivity value with the user that affects the size of the penalty resulting from failure to access the asset. When the player purchases a computer, the user will create the asset on the computer. Once it exists on a computer, attackers potentially target the asset. For example, an attacker might break into the office housing the computer and walk off with the entire computer. Or, if the asset's attacker motive is based on integrity, the attacker might hack into the computer and modify the data. If the asset is compromised, the player is penalized as specified when the designer defines the asset.

In the above example, the designer simply defines a user and an asset. The game engine manages the rest (Irvine and Thompson, 2004). The game engine manages the virtual economy to reward players when users are productive and to penalize them when goals are not achieved or assets are compromised. It also includes a sophisticated attack engine to assess the suitability of the current protection mechanisms to protect the assets based on the asset motive.

3.3. *Extending the simple scenario*

In addition to defining assets and users, the designer specifies the initial state of the scenario including:

- Physical security properties (e.g., alarms, guards, etc.) of the different zones (e.g., offices);
- The set of pre-existing computers and their configurations including network connections;
- Procedural security policies to be followed by the users;
- Initial user training (This affects adherence to procedural policies.);
- Background checks for different kinds of users (e.g., based on user clearance);
- Which kinds of attacks will be initially active and which will be suppressed;
- How much money the player will start with;
- The kinds of computers and network devices available for purchase; and
- Support staff available to help, administer and maintain computer systems.

3.4. *Interacting with the player and dynamically altering the scenario*

The CyberCIEGE scenario definition language allows scenario designers to periodically assess the ongoing game state ''conditions'' and respond using active ''triggers''. Game state conditions include such things as the passing of time, whether users are achieving their goals, computer configuration settings and whether attackers have compromised assets. Active triggers include pop-up messages, brief movies, changes in user goals, commencement of attacks, and user feedback to the player via balloon speech as reflected in Fig. 2.

Scenarios are divided into multiple phases, each of which includes one or more objectives that the player must achieve prior to moving on to the next phase. Designers use conditions and triggers to assess whether objectives have been met and to change the environment for the next phase (e.g., introduce additional user goals).

3.5. *Scenario audience selection*

The first step in the design of a scenario is to identify its purpose and audience. For example, does the intended audience have experience with computer games? Are they expected to have played other CyberCIEGE scenarios and thus have some level of mastery of the mechanics of the game?

The scenario definition language supports a broad range of different types of scenarios. At one end of the spectrum are simple scripted scenarios such as those intended for basic training and awareness. These scenarios are designed to affect user behavior where human factors are the sources for potential security compromises (Whalen, 2001), e.g., ''beware of email attachments.'' This type of scenario is often built entirely from conditions and triggers, with very little reliance on the game engines' economy or attack engines. For example, a set of conditions assess whether the user has been instructed to beware of email attachments, and triggers provide direct feedback based on that game state. At the other end are sophisticated scenarios for players who have a basic understanding of network security engineering. These scenarios rely more on the game engine itself to direct attacks and manage the overall economy.

3.6. *Elements of scenario design*

The scenario designer defines the information assets. What kind of information is it? What is the asset value and what makes it valuable? Why would an attacker target the asset? The designer also defines the users. What assets do the users need to access? Why do they need to access them? Do users need to share assets? Do users require access to assets via the Internet (e.g., publicly available documents)?

Fig. 2 – Pop-up messages can be initiated using active triggers.

The scenario designer describes the story line in the scenario briefing and in the descriptions of the assets and users. This textual information is intended to provide players with the context of the scenario. The designer describes individual player objectives and specifies the conditions that constitute the achievement of each objective. The initial state of the scenario can be used to constrain a player's options. For example, a player can be given insufficient cash to fully secure a site until an initial set of objectives is achieved.

Finally, the designer specifies feedback to move the player along through the scenario based on current game conditions. For example, what should a user say or think if a specific goal cannot be met? The engine causes the user to wander aimlessly or violently pound on the keyboard. The designer can enhance this with specific user "thoughts" or comments that appear in bubble text. In some scenarios the designer may choose to assess the suitability of protection mechanisms using conditions and warn the player prior to the attack engine's exploitation of the vulnerability. And in other scenarios the designer will provide substantial help tips to aid the player with the mechanics of the tool. CyberCIEGE includes a rich on-line encyclopedia that can serve as context-dependent help. Ultimately the designer selects the conditions that constitute a "win" or a "loss", and provides the text to display in the respective debriefing. The encyclopedia includes several animated movie tutorials (e.g., describing malicious software) that can be launched as a part of the debriefing.

3.7. *Integrated development environment*

Designers build and modify scenarios using the *Scenario Development Tool* (SDT), which automates the syntax of the CyberCIEGE scenario definition language through the use of reusable libraries and forms having pull down menus (Johns, 2004). As is illustrated in Fig. 3, the SDT permits the designer to compile and run scenarios, and then view a formatted presentation of the resulting log (Teo, 2003). In Figs. 3 and 4 the numbered arrows indicate the sequence of interactions. The SDT performs input validation and limited consistency checking (e.g., ensuring that references to users are valid). The SDT Users Guide (CISR, 2002) includes a tutorial that walks new designers through the construction of a complete scenario. The SDT was used to construct the scenarios described below. The source for these and other scenarios is distributed with CyberCIEGE, and developers may use the SDT to alter or expand the scenarios. Upon completing development or revision of a scenario, designers use the Campaign Manager to group the scenario with other scenarios into a collection of scenarios that are to be played by students in sequence as illustrated in Fig. 4. Instructors can view summaries and details of student progress via the Campaign Analyzer as illustrated in Fig. 5.

At this point, it is possible to examine how CyberCIEGE can be applied to the training and awareness needs of a real organization, in our example, the U.S. Navy.

4. Requirements elicitation

Two factors determine the requirements for the use of CyberCIEGE as a training and awareness tool in the context of the U.S. Navy. The first is the collection of policies that mandate training and awareness activities within the Military and the Navy. This is followed by an analysis of specific topics that must be addressed.

4.1. *Current policies for IA training and awareness*

Like the other services, the U.S. Navy must adhere to laws and directives intended to cover the entire Department of Defense (DoD). This section will describe the important laws and policies that have affected Navy choices with respect to training and awareness in information assurance.

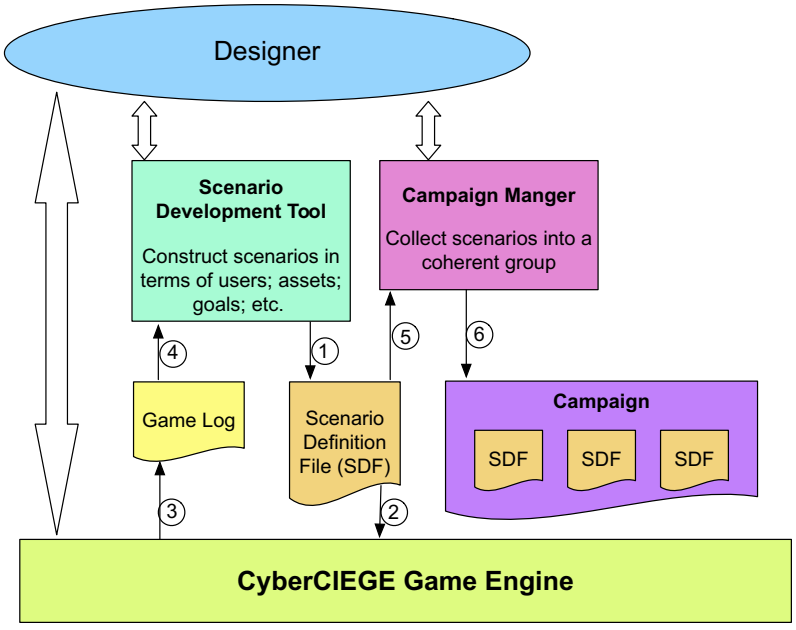

Fig. 3 – Scenario designers use the SDT and the Campaign Manager.

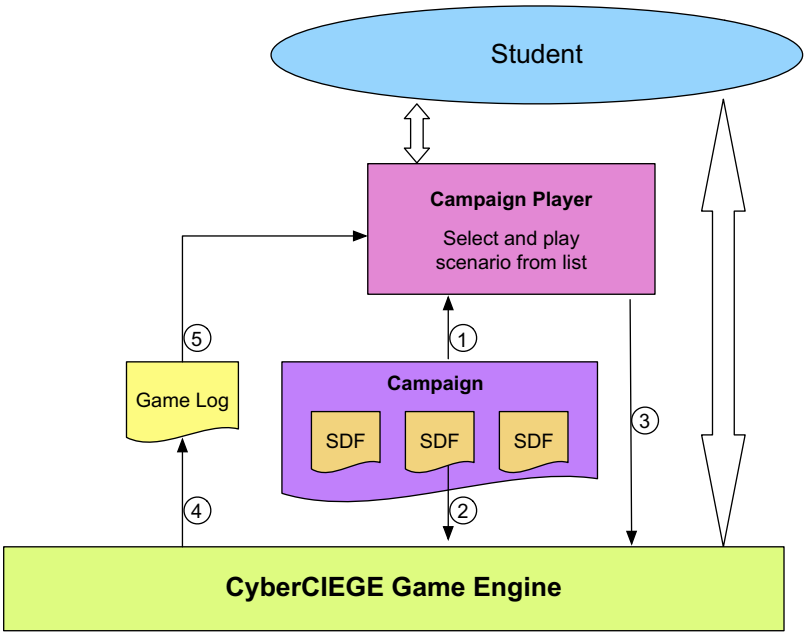

Fig. 4 – Students use the Campaign Player.

The United States Computer Security Act of 1987 mandated periodic security training for all users of Federal information systems. In response, the Department of the Navy placed the burden of responsibility for training and awareness on local Information Systems Security Managers (NSOP, 1995), who were, in turn, responsible for developing local training sessions or CBT. To supplement other IA directives (DoD, 2002, 2006), in 2004, the U.S. Department of Defense issued DoD Directive 8570.1 (DoD, 2004), which mandated initial and annual refresher information assurance training for all DoD information system users. Since then, all users of Navy information systems have been instructed to complete a DoD IA awareness CBT. The CBT is a web-enabled slide presentation. It is trivial for a personnel to click through the training to its successful completion without absorbing any of the material.

Directive 8750.1 has highlighted the importance of fostering a security culture and the need to find training techniques that will actively engage the typical user. A participatory video game requires more user involvement than slide presentations or other standard training and awareness vehicles.

4.2. *Requirements analysis*

Training and awareness requirements were developed from the legacy Information Security program of the U.S. Navy and from the current Department of Defense IA training and awareness computer-based training course.

Many of the requirements for the awareness scenario were obtained from the U.S. Navy Information Security Program. Navy requirements for user security training are found in the Navy INFOSEC program guidebooks for local Information System Security Officers (NSOP, February 1996) and Network Security Officers (NSOP, March 1996). These documents offer recommended training curriculum topics and subtopics including:

- The value of information, e.g., personnel files, legal records, and trade secrets
- Communication and computer vulnerabilities such as malicious software, Internet risks, human errors, and Internet security risks
- Basic safe computing practices such as locking computers when unattended
- Password management including password generation, protection, and change frequency
- Local security procedures, e.g., cipher locks and violation reports

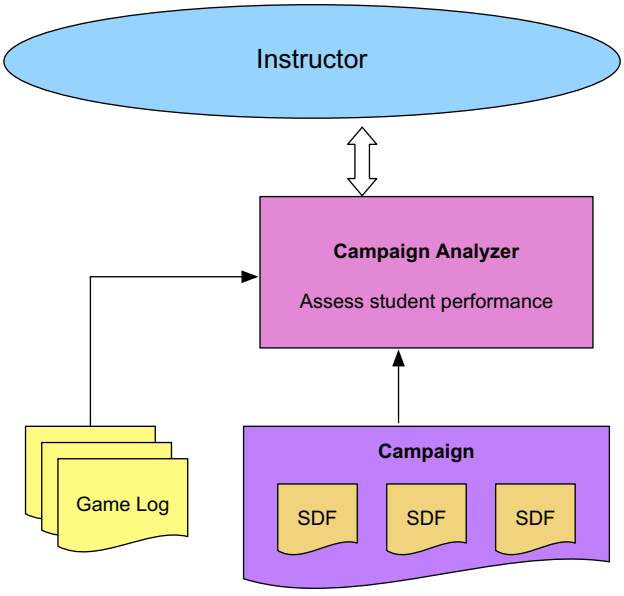

Fig. 5 – Instructors use the Campaign Analyzer.

The other requirements source was the DoD Information Assurance Awareness CBT. The majority of naval organizations currently use the "DoD Information Assurance Awareness" CBT (DoD, 2006) to fulfill obligations for enterprise-wide annual refresher training. It addresses the following topic areas:

- Importance of IA (overview, evolution, and policy)
- IA threats (threats, vulnerabilities, social engineering, and internet security)
- Malicious code (overview, protection, and internet hoaxes)
- User roles (system security and protecting DoD information)
- Personal and home security (on-line transactions and security tips)

These topics provided the requirements for the video game-based training and awareness.

5. Scenarios for training and awareness

Two CyberCIEGE scenarios were designed to fulfill the Navy IA training requirements. The first seeks to make the player aware of basic IA problems and principles. The second is intended for more sophisticated users of computer-based assets. A brief summary of other CyberCIEGE awareness and training scenarios is provided in Section 5.2.

The basic user scenario focuses on computer security fundamentals. The player is placed in the role of a security decision maker aboard a ship, who must complete objectives that raise the security posture of the organization. If objectives are not completed within a specified time, appropriate attacks are triggered by the game engine and the player is penalized. After completing each objective, the player is presented with an awareness message that relates the action taken in the game with real-life circumstances and provides feedback regarding the players choices. The player wins by completing all the objectives without incurring "fatal" penalties.

For each topic identified in the requirements analysis, a scenario element was created that requires the player to do something that will convey the concept to be learned. Some of the topics and activities are described in Table 1. Features that made this scenario Navy-specific included the protection of classified information and cultural aspects of organizational security associated with the hierarchical command structure of the DoD.

5.1. *Scenarios for IT staff*

Navy IT training requirements for staff with IT-related jobs are addressed by a second scenario that focuses on network security, and serves to introduce technical users into the roles they must assume. The player assumes the role of acting security manager while the "boss" is away. The player must manage three internal networks, one of which processes classified information. During this scenario, the player must complete technical objectives addressing physical security mechanisms, access control, filtering, antivirus protection, data backups, patching configurations, password policies, and network vulnerability assessment.

Table 1 – Basic awareness topics and player activities

Topic	Player activity
Introductory IA briefing	This briefing includes definitions and descriptions of important IA elements and how they interact.
Information value	The user must protect high value information and answer questions about information dissemination.
Access control mechanisms	The player is introduced to both mandatory and discretionary access control, with the latter as a supplement to controls on classified information.
Social engineering	The player is presented with a scenario that will lead to a social engineering attack if proper action is not taken.
Password management	The player must prevent a game character from revealing his password to an outside contractor.
Malicious software and basic safe computing	The player must determine and expend resources to procure three procedural settings that will prevent malicious software propagation.
Safeguarding data	The player is presented with a situation where it appears that a game character is leaving the premises with sensitive information. Actions taken by the player allow the importance of secure storage of backups to be conveyed.
Physical security mechanisms	The player must select cost-effective physical security mechanisms to prevent unauthorized entry into sensitive areas.

5.2. *Other scenarios*

The rich and flexible CyberCIEGE scenario definition language supports information assurance training beyond military environments. For example, an "identity theft" scenario was built to teach users about the methods of identity theft prevention in home computing environments (Ruppar, 2005). This scenario focuses on a few basic user behaviors that can greatly reduce the risk of identity theft, while highlighting consequences of risky behavior through an engaging story line.

One set of scenarios was developed solely to help train users to reduce the risks of distributing worms and viruses. Here, the player can see the damaging effects of worms and viruses, and learns that a major cause of malicious software proliferation is through user execution of email attachments.

Other CyberCIEGE scenarios illustrate more complex and subtle information assurance concepts. These longer, more sophisticated scenarios are more like traditional simulation and resource management games. For these, the target audience may be advanced computer security students, or information security decision makers.

Several students have developed relatively complex scenarios as part of their master's thesis work, an example of which is described by Fielk (2004). And while not all such efforts have resulted in polished games that are fun to play, the process of building scenarios requires students

to confront fundamental information assurance issues in order to build a consistent virtual environment. For example building a scenario requires the student to explain an asset's value to the player in a way that the player can understand both the consequences of asset compromise, and the motives of would-be attackers.

The two Navy IA training scenarios described above were completed as part of a master's thesis. Development of a basic scenario, including a substantial learning curve for the SDT, requires between 330 and 400 h of work depending on the student's aptitude and programming skills.

6. Discussion and future work

This paper demonstrates that information assurance awareness and training can be provided in an engaging format. CyberCIEGE was employed to meet a specific set of Navy IA training requirements, thus demonstrating that it is sufficiently flexible to illustrate a range of security topics in a variety of environments, both generic and organization-specific. Initial test results for the basic user training scenario are positive and illustrate the utility of CyberCIEGE in supporting awareness programs.

6.1. *User experiences*

CyberCIEGE was originally developed to be made available at no cost to organizations of the federal government of the United States. Since then, our development partner elected to also make it available at no cost to schools and universities. To date, approximately 130 organizations have made inquires at the CyberCIEGE website (CISR, 2006) and have been given download instructions. A number of these organizations currently use the game as a training tool.

The tool is used at our institution within our information assurance curriculum, and has been the subject of several master theses as described in Section 2.2.2.

These and more casual user experiences have resulted in feedback on CyberCIEGE, which has led to a number of recent improvements.

6.2. *Future work*

The effectiveness of CyberCIEGE for basic information assurance awareness has not yet been fully assessed. While initial feedback has been positive, a side-by-side comparison with traditional on-line click-through awareness programs (DoD, 2006) is needed. This testing would include a test group that only recieves CyberCIEGE training, one group that only receives click-through training and one group that receives both. Our informal experiences show that some users simply will not expend any effort to learn even the most basic mechanics of a video game. For these users, interactive training methods will not be effective if they require anything more involved that the repeated clicking of a mouse or pressing of an enter key. On the other hand, those users with some experience in video games or adventure games appear more inclined to explore the game, sometimes proceeding beyond the simple awareness scenarios into more sophisticated scenarios. A test study with a relatively large user pool would help quantify the usefulness of CyberCEIGE in place of or in addition to existing on-line awareness programs.

There are several functional aspects of CyberCIEGE for which future work is planned. First, it would be useful for instructors to be able to monitor the ongoing progress of students as they advance through either a single scenario or a campaign of several scenarios. Additional mechanisms and tools will be required in the CyberCIEGE framework to support this capability.

The ability of the scenario designer to use triggers and other dynamic mechanisms to cause changes in the evolution of a scenario is one of the greatest strengths of CyberCIEGE. Further investigation is required to determine additional techniques to introduce dynamic content in the game. In addition, the tool would benefit from better development interfaces with which to experiment with and test dynamic content.

Many video games involve multiple users and such activity is envisioned for CyberCIEGE. We have conducted a requirements analysis for a multiplayer version of CyberCIEGE and have determined how best to engage multiple players without turning it into an exercise that would give the appearance of promoting misbehavior on IT systems. Players are assumed to be concerned about partners with whom they might conduct cyber-based business interactions. To determine whether other systems are qualified to be a participant in the protection of his information assets, a player would conduct various tests on these foreign systems. The game would consist of a scenario-specific number of rounds of preparation and testing by all nodes. As with existing single-player scenarios, tests could be focused on a particular information assurance issue, such as passwords or firewall configuration, or could cover a broad range of topics.

CyberCIEGE is currently designed to address wired networks. A more advanced version of the game could include both wired and wireless platforms. For the latter, issues associated with user and platform mobility, platform resources, wireless authentication, etc. could be addressed. In addition, CyberCIEGE could anticipate the security challenges that will be encountered in the next generation of processors. These include the management of virtual machine monitors and their guest operating systems in virtual machines, platform monitoring and attestation, distributed system management, and the balance between corporate convenience and individual privacy.

Acknowledgments

This work has been supported by the United States Navy, by the Department of Defense, and by the Office of Naval Research. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not reflect the views the US Navy, Department of Defense, or the Office of Naval Research.

REFERENCES

de Aguilera M, Mendiz A. Video games and education: (education in the face of a "parallel school"). Computers in Entertainment 2003;1(1):1–10.

Bell DE, LaPadula L. Secure computer system unified exposition and multics interpretation. Technical Report ESD-TR-75-306. Hanscom AFB, MA: MITRE Corp.; 1975.

Biba KJ. Integrity considerations for secure computer systems, Technical Report ESD-TR-76-372. MITRE Corp.; 1977.

Bishop M. Computer security: art and science. Reading, Massachusetts: Addison-Wesley; 2002.

CISR. CyberCIEGE scenario development tool users guide march. Monterey, CA: Naval Postgraduate School; March 2006.

CISR. CyberCIEGE, <http://cisr.nps.edu/cyberciege/>; 2002.

Central Coast Security. Security awareness/motivation posters, <http://members.impulse.net/~sate/posters.html#CompuSec>; September 2006 [Last accessed 11 September 2006].

DoD Directive 8500.1. Information assurance; 24 October 2002. Available from: <http://www.dtic.mil/whs/directives/corres/html/85001.htm> [Last accessed 20 June 2006].

DoD Directive 8570.1. Information assurance training, certification, and workforce management; 15 August 2004. Available from: <http://www.dtic.mil/whs/directives/corres/html/85701.htm> [Last accessed 20 June 2006].

Executive Office of the President. The national strategy to secure cyberspace. Available from: <http://www.whitehouse.gov/pcipb/>; 2003 [Last accessed 15 September 2006].

Fielk KW, CyberCIEGE scenario illustrating integrity risks to a military-like facility. Masters thesis. Monterey, CA: Naval Postgraduate School; September 2004.

Foreman J. Video game studies and the emerging instructional revolution. Innovate(1), http://www.innovateonline.info/, 2004;1 [Last accessed May 2006].

Gee JP. What video games have to teach us about learning and literacy. Plagrave Macmillan; 2003.

Gee JP. What would a state of the art instructional video game look like? Innovate(6), http://www.innovateonline.info/, 2005; 1 [Last accessed May 2006].

Gredler ME. Games and simulations and their relationships to learning. In: Handbook of research on educational communications and technology. 2nd ed. Mahwah, NJ: Lawrence Erlbaum Associates; 2004. p. 571–81.

Irvine CE, Thompson MF. Teaching objectives of a simulation game for computer security. In: Proceedings of informing science and information technology joint conference, Pori, Finland; June 2003. p. 779–791.

Irvine CE, Thompson MF. Expressing an information security policy within a security simulation game. In: Proceedings of the sixth workshop on education in computer security. Monterey, CA: Naval Postgraduate School; July 2004. p. 43–9.

Irvine CE, Thompson MF, Allen K. CyberCIEGE: an information assurance teaching tool for training and awareness. In: Federal information systems security educators' association conference, North Bethesda, MD;March 2005.

Irvine CE, Thompson MF, Allen K. CyberCIEGE: an extensible tool for information assurance education. In: Proceedings of ninth colloquium for information systems security education, Atlanta, GA; June 2005. p. 130–138.

Johns KW. Toward managing and automating CyberCIEGE scenario definition file creation. Masters thesis, Monterey, CA: Naval Postgraduate School; June 2004.

Lunt TF. Access control policies: some unanswered questions. Computers and Security 1989;8(1):43–54.

Nexus Interactive. AI Wars: the awakening, <http://www.aiwars.com>; 2003 [Last accessed November 2003].

National Institute of Standards and Technology. People: an important asset in computer security. NIST-CSL Bulletin October 1993.

Information systems security manager (ISSM) guidebook. Navy Staff Office Pub. 5239-04; 1995.

Information systems security officer (ISSO) guidebook. Navy Staff Office Pub. 5239-0; February 1996.

Network security officer (NSO) guidebook. Navy Staff Office Pub. 5239-08; March 1996.

Prenski M. Digital game-based learning. New York: McGraw-Hill; 2001.

Roberts IE, McColgin DW, Greitzer FL, Huston K. Usability and training effectiveness evaluation of CyberCIEGE. Pacific Northwest National Laboratory; January 2006.

Ruppar C. Identity theft prevention in CyberCIEGE. Masters thesis, Monterey, CA: Naval Postgraduate School; December 2005.

Squire K. Changing the game: what happens when video games enter the classroom? Innovate(6), http://www.innovateonline.info/, 2005;1 [Last accessed May 2006].

Teo TL. Scenario selection and student selection modules for CyberCIEGE. Masters thesis, Monterey, CA: Naval Postgraduate School; December 2003.

U.S. Department of Defense: Defense Information Systems Agency. CyberProtect, version 1.1. DoD IA training and awareness products, <http://iase.disa.mil/eta/prod-des.html> July 1999 [Last accessed 17 June 2006].

U.S. Department of Defense: Defense Information Systems Agency. DoD information assurance awareness course, <http://iase.disa.mil/dodiaa/launchPage.htm> February 2006 [Last accessed 11 September 2006].

Whalen T. Human factors in coast guard computer security – an analysis of the USCG's current awareness level and potential techniques to improve security program viability. Masters thesis, Monterey, CA: Naval Postgraduate School; June 2001.

Benjamin D. Cone is a Lieutenant in the United States Navy. He holds a B.S. from the United States Naval Academy, Annapolis, Maryland, and a M.S. in Information Technology Management from the Naval Postgraduate School in Monterey, California. Since graduation he has been at sea.

Cynthia E. Irvine is a Professor in the Department of Computer Science at the Naval Postgraduate School in Monterey, California. She holds a B.A. in physics from Rice University and a Ph.D. in astronomy from Case Western Reserve University, Cleveland, Ohio. Her fields of interest include inherently trustworthy systems, security architectures, and security education.

Michael F. Thompson is a Research Associate in the Center for Information Systems Security Studies and Research at the Naval Postgraduate School in Monterey, California. He also serves as Lead Security Engineer for Aesec Corporation. He holds a B.S. in Electrical Engineering from Marquette University. His research interests include security engineering and highly secure systems.

Thuy D. Nguyen is a Research Associate in the Department of Computer Science at the Naval Postgraduate School in Monterey, California. She holds a B.S. in Computer Science from the University of California at San Diego. Her research interests are high assurance systems, security engineering, and security requirements elicitation.