Proceedings of the 2003 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY June 2001

A Security Simulation Game Scenario Definition Language

Naomi Falby[*], Michael F. Thompson[*], and Cynthia E. Irvine[*], *Senior Member, IEEE*

Index terms – Information Assurance, Simulation Game, Scenario Definition Language, Education

EXTENDED ABSTRACT

The Center for the Information Systems Studies and Research (CISR) at the Naval Postgraduate School has established a broad program in computer and network security education. The program, founded on a core in traditional computer science, is extended by a progression of specialized courses and a broad set of information assurance research projects. A CISR objective has been improvement of information assurance education and training for the U.S. military and government. Pursuant to that objective, CISR is developing a computer simulation game, *CyberCIEGE*, to teach computer security principles. CyberCIEGE players construct computer networks and make choices affecting the ability of these networks and the game's virtual users to protect valuable assets from attack by both vandals and well-motivated professionals [1].

A key CyberCIEGE innovative is a *scenario definition language* that permits educators to generate many different security scenarios, each playable as an independent game. Every scenario includes a briefing that describes an enterprise (e.g., a business that depends on the secrecy of proprietary information) and gives the player information about what must be done to help make the enterprise successful. The scenario language is used to define a set of *users* and *assets*. Users are typically enterprise employees whose productive work makes money for the enterprise. Assets are various kinds of information required for user productivity. Example assets are secret formulas, accounting information, business plans, expense statements, and marketing material. Using the language, the scenario designer can define a number of different users who each need to access different assets in different ways to support enterprise productivity. These are user *goals*. The language can express the need for users to share assets and to access multiple different assets concurrently. Different assets have different values, and different users have different authorizations to access assets as defined by the enterprise security policy. Additionally, each asset has a value to *attackers* distinct from its value to the enterprise. This permits the scenario designer to express the motives that will drive virtual attackers in their attempts to compromise assets.

The users, assets, user goals and enterprise security policy are established by the scenario designer using the language, and may not be changed by the player. Additionally, the scenario designer can define a set of computer components (e.g., workstation, servers, firewalls, etc.) that the player can purchase and configure to support their virtual users' goals. The scenario designer also defines the networks, (including the Internet), available to the player for interconnecting components. Furthermore the scenario designer can define a set of security personnel (e.g., guards) and support staff that the player can hire to help enforce physical security policies and maintain component and network configurations.

The scenario designer specifies the costs of the various resources (e.g., workstation price, guard salary), and the effect of user goals on productivity and happiness. This results in the fundamental tension of computer security: Provide users with suitable resources to productively perform work while protecting the assets from security compromises in accordance with the enterprise security policy.

REFERENCES

[1] 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.

Naval Postgraduate School, Monterey, California. This material is based upon work supported by NETC and OSD. Opinions, findings, and conclusions expressed in this material are those of the authors and do not necessarily reflect those of the sponsors.

ISBN 555555555/$10.00 © 2003 IEEE