2006

The Cyberciege Information Assurance Virtual Laboratory

Thompson, Mike

http://hdl.handle.net/10945/49137

THE CYBERCIEGE INFORMATION ASSURANCE VIRTUAL LABORATORY

Mike Thompson

Naval Postgraduate School

Abstract: CyberCIEGE enhances information assurance education and training through the use of computer gaming techniques. In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack. These tutorial sessions will introduce CyberCIEGE to educators and information assurance training professionals. The IA training tool is provide to develop new scenarios.

Key words: Information Assurance, Education, Simulation, Virtual World

The CyberCIEGE project creates an Information Assurance (IA) teaching/learning laboratory. In addition to rigorous scientific foundations, it involves the application of abstract principles to the real world. A hands-on virtual laboratory provides a dynamic and often surprising context where abstract principles can be applied and discovered.

CyberCIEGE is an innovative computer-based tool to teach network security concepts. The tool enhances information assurance education and training through the use of computer gaming techniques such as those employed in SimCity™ and RollerCoaster Tycoon®. In the CyberCIEGE virtual world, users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack.

In its interactive environment, CyberCIEGE covers the significant aspects of network management and defense. Users purchase and configure workstations, servers, operating systems, applications, and network devices. They make tradeoffs and prioritization decisions as they struggle to maintain the ideal balance between budget, productivity, and security. In its longer scenarios, users advance through a series of stages and must protect increasingly valuable corporate assets against escalating attacks.

The CyberCIEGE encyclopedia of security concepts contains a wealth of information assurance knowledge. Users can read the encyclopedia, or watch its instructional movies!

CyberCIEGE supports many educational venues, from basic workforce awareness training to university classes. It can help organizations meet DoD Directive 8570 obligations for IA training, annual IA awareness refreshers, and appropriate IA education. CyberCIEGE contains support for the creation of tools to record and assess student progress. Best of all, CyberCIEGE is extensible.

CyberCIEGE includes a language for describing its security scenarios. Using this language, educators may construct or modify scenarios that can then be played by students. CyberCIEGE was created by the Center for Information Systems Security Studies and Research (CISR) at NPS, and Rivermind, Inc., of San Mateo, CA.

1. WECS CYBERCIEGE INFORMATION ASSURANCE TRAINING TOOL TUTORIAL

These tutorial sessions will introduce CyberCIEGE to educators and information assurance training professionals. A hands-on laboratory will allow participants to explore the IA training tool and learn to develop their own scenarios. Participants will receive a copy of CyberCIEGE for their own use. Workshop topics include:

I. Introduction to CyberCIEGE
  Central concepts and abstractions
  Tool navigation and scenario demonstration
  Hands on play of a CyberCIEGE scenario

II. Strategies for deploying CyberCIEGE for training and education
  Simple scripted training scenarios
  Virtual setting immersion scenarios
  Assessing student progress using automated log analysis

III. Development and enhancement of CyberCIEGE scenarios
  Use of the Scenario Development Tool
  Tutorial to develop a simple new scenario
  Understanding CyberCIEGE virtual attackers motivations and means
  Reliance on game engine behavior vs. scripting scenarios with conditions and triggers
  Story telling to engage the player¹s emotions
  Packaging multiple scenarios into a single campaign