Active Learning with the CyberCIEGE Video Game

Michael F. Thompson and Dr. Cynthia E. Irvine
Department of Computer Science
Naval Postgraduate School
Monterey, CA USA
The CyberCIEGE Educational Video Game

- Educational tool for teaching cyber security
  - Developed by NPS via several government sponsors
  - Used by universities, community colleges, & government

- Players construct and defend computer networks
  - 3D “construction & management simulation” video game
  - Many scenarios illustrating a range of security topics

- Custom-built game engine manages attacks and economy
  - Enterprise assets and users who need to access assets
  - Attacks driven by motive: malware; flaws; insiders; etc.
Educational Goals

• Broad audience
  - Cover a wide variety of computer security concepts
  - Relatively low barrier to entry beyond basic game mechanics

• Let students approach the game on their terms
  - Try “wrong” choices, experiment, fail, reflect
  - Stand alone game hosted on standard platform (windows)
  - Game available in computer labs and for use on own laptops

• Primarily a teaching (vice testing) tool
CyberCIEGE Components

• Domain-specific simulation engine packaged as a game
  - Network topology and security assessment
  - Game economy and motive-driven attacks

• Scenario definition language
  - Express a range of scenarios
  - Simple training & awareness through cyber-warfare

• Video-enhanced encyclopedia
  - Animated tutorial videos
  - Player help and lab manuals

• Student assessment tool
  - Detailed game logs reflecting student choices
  - Summary reports showing student progress
Network Simulation

• Illustrate fundamental computer security concepts
  - Configurable components; meaningful player choices
  - Experience consequences of choices

• Not a high fidelity vulnerability analysis tool
  - Abstract representation of security products and features
  - Avoids much of the configuration minutia; focus on function

• Attack engine
  - Network topology and configuration assessment
  - Insiders; trap doors; wiretaps; physical security; etc.
Hands on Experimentation with Security Concepts

• Scenario-specific Policies: Users and Information (assets)
  - User (character) goals to access assets
  - Attacker motives to compromise assets

• Things the player can change:
  - Physical Security: guards; locks; biometrics; access lists
  - Component configuration (e.g., ACLs; filters; VPNs; etc.)
  - Procedures (user behavior depends on policy/training)
  - Patch management; configuration management; etc.
  - Network topology: air gaps; vulnerable network links
  - PKI used for VPNs, email and SSL/TLS
  - Personnel security: background checks; malicious insiders
Game Engine Attacks: Motives Determine Strength

- Direct and indirect access by outside attackers
  - May require entering a physical zone
  - Trojan horses; trap doors; flaws; configuration errors
  - Procedures (external software, user training, CM, etc.)
  - Separate Internet attacks
- Insiders
  - Like outsiders, but based on trust (background checks)
  - May be bribed to disclose / modify assets directly
- Wiretaps (viewing & modifying bits on the wire)
- Other
  - Compromises of PKI elements (e.g., subverted CA)
  - Smart cards as a medium for data flow
Workstation and Server Components

• Operating Systems
  - Access control lists
  - Label based mandatory access controls
  - Authentication, password policies; auth servers, biometrics

• Configure application based security
  - SSL / TLS on servers (web servers; SSH servers)
  - Email encryption; browsers; SSH clients; VPN clients

• Varying assurance and patch requirements
  - High motive attacks require high assurance platforms
Networking Components

• Routers
  - Simple interconnection of networks. No network addressing
  - Configurable application service filters (firewall).

• VPN Gateways (clients are similar)
  - Symmetric key or public key (PKI)
  - “Connection Profiles” define traffic protection types
  - Illustrates risks, e.g., “island hopping”
  - Clients configurable for “measured boot” (like a TPM)

• Link Encryptors
  - Manual key management vs software-based
  - Won’t work through routers
Sample Game Play

- CyberCIEGE Network Filters scenario

Larry wants you to meet his on-line "date" ... ...but you better first check your new objectives...
**NPS Experience with CyberCIEGE**

- Scenarios assigned as labs for Intro to Computer Security
  - Students receive full period of introduction and group play
  - Included in course for nineteen quarters

- No formal NPS research, pilot studies at two institutions

- Based on informal feedback and observations of logs:
  - Most students enjoy the game and have learned from it
  - Students approach games in a variety of different ways

- Key adaptations based on our experience
  - Feedback for a broader set of player choices: MORE HELP
  - In-game formative assessment (e.g., multiple choice)
Time Spent on the Filters Scenario (149 students)

![Bar graph showing the time spent by 149 students on the filters scenario. The x-axis represents the total minutes per student, ranging from 5 to 75 minutes. The y-axis represents the number of students, ranging from 0 to 25. The data is organized into bars, with the highest number of students spending between 30 and 35 minutes.](image-url)
Filters Scenario Sessions Started (149 students)
Current and Future Work

- NPS is working with NSF to adapt CyberCIEGE
  - Further align with standard computer security textbooks
  - Additional focus on network parameter, e.g., packet analysis
  - Ultimate objective: to use in formal education settings

- A need for formal education research
  - Are games an effective way to teach?
    - In the class room; in the lab; as homework?
    - Is there a measurable difference from other techniques?
  - Seeking education research collaborators
Conclusion

• Hands-on exercises promote active learning
• Computer security is a good target for serious games
  - Sometimes subtle concepts
  - Simulate complex environments and extreme consequences
• Effectiveness of serious games needs formal research
  - CyberCIEGE has good depth of material
  - Hundreds of universities and community colleges
• CyberCIEGE is available with a no-cost educational license
  - Email cyberciege@nps.edu
  - SDK available for customizing scenarios
Contact

Cynthia E. Irvine, Ph.D
Professor and Director
irvine@nps.edu

Michael F. Thompson
Research Associate
mfthomps@nps.edu

Center for Information Systems Security Studies and Research
Department of Computer Science
Naval Postgraduate School, Monterey, CA  93943
U.S.A

http://www.cISR.us