The SimSecurity Information Assurance Virtual Laboratory

Cynthia E. Irvine
Center for INFOSEC Studies and Research
Naval Postgraduate School

The purpose of the *SimSecurity* project[1] is to create 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.

SimSecurity will package the information assurance laboratory as an interactive, entertaining, commercial-grade PC-based computer game where players assume or observe various roles involved in attacking and defending a networked computing system (e.g., manager, system administrator, system user, attacker). Students will interact with others actors in the environment, operate and configure information systems, and defend those systems. The laboratory will adapt to the decisions, omissions, and strategies of students, indicating effects via built-in resource limitations and various enterprise success factors. Students will be able to visualize, not only their actions in the environment, but also how others see those actions, and the consequences of those actions.

Over forty scenarios have been created that depict environments ranging from those of home users to large distributed enterprises. These scenarios are used by the underlying game engine to create game instances. The game-engine architecture facilitates the addition of feature extensions as new threats and countermeasures in the real world IA landscape evolve. This extensibility allows researchers and instructors to upgrade the simulation capabilities without invalidating earlier components, thereby enabling rapid, continuous, and relatively inexpensive updates.

The laboratory can be used in three different modes. The first is a stand-alone ad hoc game, to teach users basic IA concepts and vocabulary. The second is a self-paced tutorial; this mode can be used as an introduction to IA concepts or to reinforce previous training and education. The third mode combines the laboratory with a course: students navigate through the IA lab in a systematic instructor-defined program. When used in conjunction with NPS learning modules and courses, students may progress through a sequence of labs and lectures to a NSTISSC-based certification and/or course credit from NPS. The interactive environment is intended to provide an exciting setting that stimulates learning and reinforces abstract principles taught in classrooms or books.

The initial version of SimSecurity will be restricted to single players. A subsequent version permitting multiple players and advanced scenarios based on the use of mobile computing resources is planned. Our intent is to construct the laboratory such that it can be tailored to particular teaching objectives and will present interfaces that can be used to add supplementary educational materials as well as student assessment tools. Whether the significant investment to provide a commercial game experience results in a high payoff in education, training, and awareness regarding information assurance concepts will be the subject of additional research following its release.

---

[1] The project is currently funded by CNET, Office of Chief of Naval Operations (CNO-N6), and the Office of the Secretary of Defense.