Title:

Simulation Approaches in Information Security Education

Author, presenter and all contact points:

John H. Saunders, Ph.D., GSEC
Voice (202) 685-2078, FAX (202) 685-3974
Information Resources Management College, National Defense University,
198 Marshall Hall, Fort Lesley J. McNair, Washington, DC 20319-5066,
saunders@ndu.edu

Abstract

This paper and presentation provides a look at instructional methods for information assurance (IA) using simulation. The simulation methods of 1) Packet Wars, 2) Sniffers + Network Design Tools, 3) Canned Attack/Defend Scenarios, 4) Management Flight Simulators, and 5) Role-playing are presented. These techniques are presented as options for educating a variety of IA constituency including network administrators, functional managers, security managers, and naïve users. Each method is demonstrated and its value supported by providing examples and by drawing upon conclusions from the author's experiences using them in a classroom environment.

The session looks at simulation as a foundation for providing benefits in understanding computer security by;

- Providing a long term view of security,
- Demonstrating a balancing act of data, program, and network access versus restriction,
- Presenting a competition for limited defensive resources,
- Involving cooperation from a variety of players, and
- Staging an analysis of risk tradeoffs.

The presentation involves participation in group simulation exercises.

Simulation Approaches in Information Security Education

John H. Saunders, Ph.D., GSEC
Information Resources Management College, National Defense University
198 Marshall Hall, Fort Lesley J. McNair, Washington, DC 20319-5066
saunders@ndu.edu

Introduction

Learning information security presents a challenge for the student no matter what his or her background may be. For a naïve user, the myriad of new terminology and an assumed understanding of basics such as networking and software execution provide a daunting hurdle. For the manager, whether technically savvy or not, the tendency to slide into irrelevant detail never seems to fade. And for the system administrator, the pull between providing system access, while also maintaining security, tests their ability to foresee the consequences of their actions.

At the same time, individuals within the different levels of the organization must respond in different ways to a crisis or to the planning of InfoSec defenses. Whereas a CIO may need to practice the process of calling in the services of an emergency backup facility, a network engineer may need to simulate when it is prudent to shut down the internet connection. And the security design engineer may need to better understand which features on an Intrusion Detection System (IDS) operate best within a specific data environment. The table below presents a sample of those types of questions being asked about information security in every organization.

Area of Focus	Level	Questions	Model Entities
Personnel Hiring/firing/turnover Training Productivity	Operational, Strategic	• Is the lag time for the acquisition of security personnel adequate? • Are our people on average performing adequately, well trained? • Is the flow of work well designed? • How will a crisis action flow with our contingency provider?	People, Dollars, Morale, Experience
Finance Budget Acquisition Supply Chain	Strategic	• Will our budget flow meet our requirements? • What scenarios can justify needed contingency funding? • How might we streamline our CERT processes?	Dollars, Units of Product, Risk Measures
Technology Computer Hardware Network Connects Software Databases	Operational, Tactical	• How should we exercise our system to insure that, for surge requirements, our computers are fast enough and our communications lines are adequate? • Is the security element in our software development proceeding well? • Given known attacks how will our network react?	Computers, Routers, Lines of Code, Connectivity, Transactions, Incidents

Creating and exercising a system to learn more about the possible answers to these questions is exactly the type of process that simulations are meant to serve. These questions cannot be answered without using a method such as simulation to;

- See the <u>long term system view</u>,

- Understand the intertwined balancing act of the controllable and uncontrollable variables in security,
- Appreciate the offensive/defensive nature of the resource equation,
- Experience the cooperation among the many organizational players, and
- Witness the analysis of the risk tradeoffs.

Through simulation exercises, responses to these questions can be learned. ***It is too late to formulate a proper response after the crisis has occurred or after the system has failed to perform***. If the team players have an opportunity to repeatedly rehearse their roles, then the stage performance, even with the element of surprise, becomes much more manageable. Further, simulation can be utilized effectively across a wide berth of areas in information security such as:

- Research and development of new countermeasures,
- Testing of both attacks and defenses,
- Production level fielding of countermeasures,
- Analysis of intrusions and attacks, and
- Education and training.

Specific Benefits of Simulation

Certainly the Information security community demonstrates a need for a modeling and simulation capability. Attacking your own system as an educational exercise is a foolish option. It has led to prison time for some individuals. As Fred Cohen [1999] has stated "The high cost of running real-world attacks, the limited extent to which they exercise the space of actual attacks, and the high potential for harm from a successful attack conspire to make some other means of analysis an imperative."

The benefits of simulation in the security arena are numerous. Some are outlined in the figure below.

- Instant "reset" of computers, networks, etc to initial conditions
- Compression of long term activity into short periods
- Lower cost than utilizing real computers, networks, software, protocols, etc
- Ease of scalability
- Creation of scenarios too risky for "real world" testing
- Levels of abstraction like the OSI model may be represented
- Ease of re-configuration
- Capability for building in an "automatic/scripted" Black or White Team

Given that the creation of security models and simulations has real benefit to the community, what sort of simulations and events have already taken place within this realm, and what might we expect to arise in the near future?

Simulations/Exercises in the Information security Arena

There are many examples where simulation has already served the information security community. For purposes of description and analysis, the examples provided here have been divided into 1) Packet Wars, 2) Sniffers + Network Design Tools, 3) Canned Attack/Defend Scenarios, 4) Management Flight Simulators, and 5) Role-playing. There are other taxonomies that could be utilized such as that used by IATAC for classifying types of M&S tools [Wagg, 2001]. But it was felt by the author that the taxonomy proposed above would best serve the practitioner for making a decision about the level of effort they would need to extend to get started in this arena.

Packet Wars

This type of simulation involves tactical level network attack and defense. These types of simulations exist for technical personnel primarily on the local network or at best enterprise level. The primary mode to date has been to set up real, but isolated, networks with servers, clients, and switching/routing equipment. Likely the best example of an academic lab exists at the United States Military Academy (USMA) in West Point, New York. It is called the Information Warfare Analysis and Research (IWAR) Laboratory [Schafer, 2000]. A diagram of their network can be seen below.

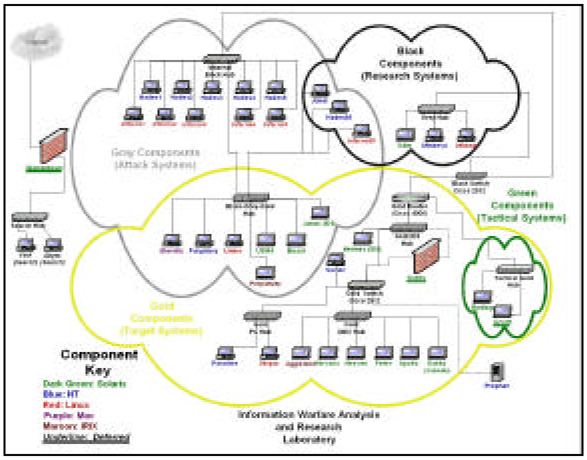

Black Components (Research Systems)
Gray Components (Attack Systems)
Green Components (Tactical Systems)
Gold Components (Target Systems)
Component Key
Dark Green: Solaris
Blue: NT
Red: Linux
Purple: Mac
Maroon: IRIX
Underline: Defered
Information Warfare Analysis and Research Laboratory

Figure 1 - Academic Security Network at US Military Academy

The USMA has been using the lab in upper level computer science courses to educate their students in the science and art of network attack and defense. In the Spring of 2001 the military faculty at West Point worked with the faculty at the U.S. Air Force Academy and the US Coast Guard Academy to initiate an annual competition, judged by experts at the National Security Agency. As part of the competition, the students spent a semester learning about attacks and defenses. They then established defense postures for isolated networks at their facilities, and finally participated in fending off attacks from experts at NSA attempting to scan and attack the weak points in their systems Similar networks and exercises exist at Texas A&M [Hill, 2000], and Idaho State.

Other examples of these types of simulations include an annual competition run by SANs called *ID'ed Net* [SANS, 2001], the competition held each year at DEFCON, and *Rootwars* at Toorcon [Toorcon, 2001]. These types of competitions are likely the best possible approach toward simulating network attacks and defenses on the technology level. The drawbacks are obvious. Building systems solely for these kinds of exercises is very expensive and time consuming. And maintaining the system requires a large allocation of resources. Each time an exercise is run, the network must be returned to its original state. Is it possible to gain a great deal of the essence of packet wars without the resource intensive nature of the approach?

Sniffers + Network Design Tools

What simulation tools are available for professional system administrators and application designers who need models for a detail understanding and in-depth analysis of items such as packet flows, buffer overflow, and operating system compromise? One area of promise for this group is in the growth of Network Modeling & Simulation (NMS) Packages. These packages, when paired with sniffer data can provide "real" network visualization from nanosecond in-depth tracing to month long summary statistical data. NMS packages, which continue to grow in popularity and maturity, provide interesting and valuable insight into the details and the statistical analysis of network traffic. Originally crafted as tools for large-scale network design, their capabilities have been growing to allow the creation of hypothetical scenarios down to the bit level. They could be utilized for a variety of tasks related to information security such as,

- modeling server and router availability,
- testing “What ifs” on host firewall or authentication servers loads, or
- gaining insight on "unusual" network traffic.

Some packages available in this area are provided in the table below.

Name	Company	Price	Contact	Comments
Cnet	Univ Western Australia	Free	www.cs.uwa.edu.au/cnet/	Good learning tool
EcoPredictor	Compuware	$24,500	(800) 521-9353 www.compuware.com	
IT DecisionGuru	Opnet Technologies	Start at $19,000	(202) 364-4700 www.mil3.com	Significant contracts with DoD
NetCracker	NetCracker Technology	starts at $7,500	(800) 477-5785 www.netcracker.com	
NetRule	Analytical Engines	starts at $7,500	(703) 287-8720 www.analyticalengines.com	Gathering awards

The method for utilizing these tools in the security arena requires that data first be collected from the operational network. The obvious drawback is that even a short-term sample can yield gigabytes or even terabytes of data.

There are drawbacks to utilizing Network Modeling and Simulation Packages. They include:

- There is no "built-in" representation of the software execution.
- Vendors are now only beginning to focus on memory resident processes.
- No "soft" factors representation is available, e.g. how do you represent social engineering or the level of training of your people?
- The user interface is geared toward network engineering.

To overcome these resource hurdles, some organizations have focused upon building "ready, out of the box" simulations.

Canned Attack/Defend Scenarios

These simulations are typically standalone applications that can be utilized in a game like manner to facilitate learning. Individuals, who are trained in IT, but not yet conversant in finer points specific to information security, would most often use these simulations. These packages are built using Multimedia tools such as Macromedia's Authorware or Microsoft's Visual Basic, and can be packaged all on one CD. Therefore, once built, they are very easy to distribute. Up front costs for building these types of simulations can be very high. A common metric in the multimedia area is 300 man-hours of work for one hour of packaged CD activity. Another constraint is that fixed paths that must be built into the simulation. Typically a procedural, decision tree type of approach is utilized to guide the user through the simulation. Some random elements may be programmed into the scenarios, but always from a fixed set of attacks and defenses viewpoint.

Some examples from this arena include InfoChess, CyberProtect, and the Information Security War gaming System.

InfoChess, recently computerized, is focused on Military Information Operations and stems from the board game [InfoChess, 2001]. A few "specialized" rules are added to the usual game of Chess to simulate some of the characteristics of Information Operations such as "psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities." It is played by many of the Information Warfare groups within the U.S. Military. InfoChess can only be purchased with the formal instructor training. It starts at around $2500.

CyberProtect is a simulation that was built under contract by the Defense Information Systems Agency. It revolves around the purchase and application of information security countermeasures in a local area network environment. It takes place over 4 quarters. Each quarter the user makes decisions about what resources/ countermeasures to purchase and put in place. After making those decisions the simulation is set in motion. The user is then subject to a variety of security attacks. The following cycle is repeated four times:

- Purchase information security resources to apply to your network. These resources include Training, Redundant systems, Access control, Virus protection, Backup, Disconnect, Encryption, Firewalls, and Intrusion detection. The user is provided limited resource dollars to apply.

- Apply/install those resources. The user drags and drops the countermeasures to specific locations on the network. See the exhibit below for a diagram of the network.

- Experience attacks. There are nine possible forms of attack. They include Jamming, Viruses, Moles, Social Engineering, Packet Sniffers, Data theft, Data modification, Flooding, and Imitation/Spoofing. The numbers and types of attacks are random; they come from outside and inside your organization. A user might receive one attack or six. The simulation provides feedback on the nature and effects of the attack and whether the user was successful in defense of his network.

- Receive a report indicating performance level. Each quarter the user receives a score sheet based upon how well they did in purchasing and applying resources to thwart the attacks.

To successfully complete the simulation, meeting a "commanders" goal, the user needs to score a 90 or above. As in real world situations, there is good and bad fortune associated with the simulation. A user might do very poorly in allocating his resources, yet through good fortune be subject to very few attacks. On the other end of the spectrum, he might do a pretty good job in allocating the resources, yet receive numerous attacks. Even with perfect "known" defenses, the enemy may still slip through. The CyberProtect CD is distributed free of charge to qualified government personnel. This simulation has been used extensively in Technical Management level courses at the National Defense University. Some comments from students follow below.

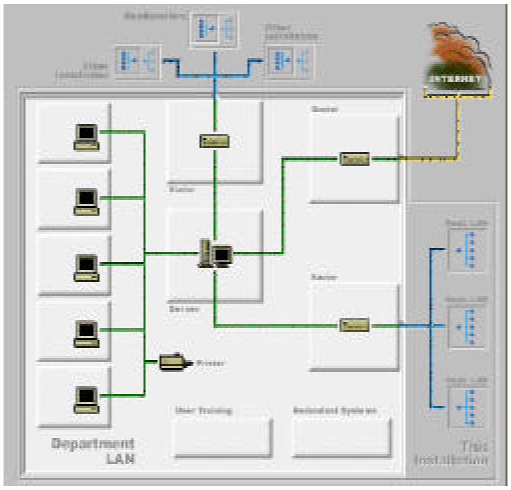


Figure 2 - Cyber Protect Network

“Overall, hands-on allows the students to understand the process. There were issues that were raised that provoked questions.....the whole purpose of the exercise.”

“It felt real; programs got stale and needed updating. It exploited where I was weak.”

“When using the tool, one would quickly find that if you did not at least cover your bases you were exposed and open to attacks. This did not mean you had to purchase the high-end tools, but strategically placing low end items were the network could handle it, and balancing between the middle to high ranges. Upgrades could be applied if funds were available later on.”

The Information Security War Gaming System (ISWGS) is a tutorial type simulation that provides a more in depth focus on specific attack types and defenses. The attacks are portrayed pictorially using a multimedia package. That is, gross packet flow is shown along with specific targets and defenses. ISWGS is also distributed free of charge to students at the IRM College at the National Defense University and to NSA Centers of Academic Excellence in Information Assurance Education.

Other interesting examples in this arena include Cohen's unnamed simulation [Cohen, 1999], and a number of others itemized in Modeling and Simulation for Information Assurance [Waag, 2001].

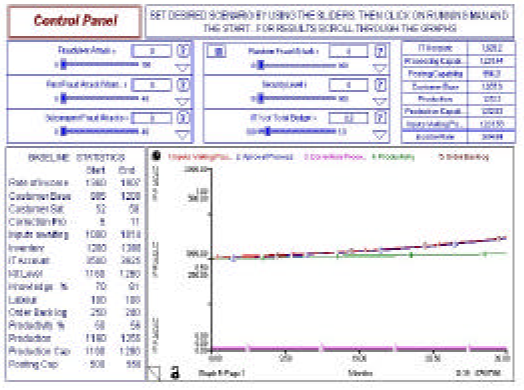
The simulations we have covered in this paper to this point have been aimed largely at the system administrator and technical manager level. What about more macro level simulations for use by managers, who need to be concerned with other factors such as budget and staffing or for learning by individuals less familiar with the details of information security? Canned simulations provide interesting training tools, but the simulations are "locked in" when shipped. What about the user who would like to play "what if" scenarios with the simulation variables? An interesting option for simulation in this area is the "micro world" or “management flight simulator."

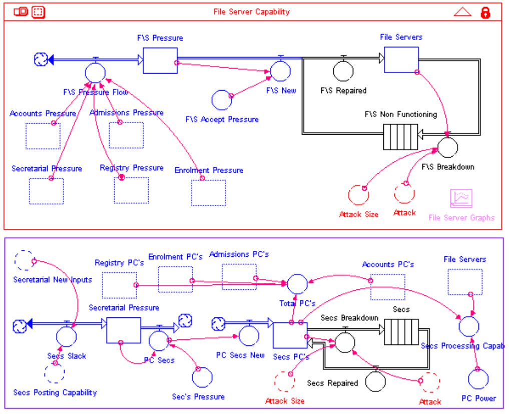
Management Flight Simulators (MFS)

These applications are built using a System Dynamics or a Discrete Event simulation tool. System Dynamics is a technology that uses difference equations to simulate the changing state of quantities and flows through multiple time periods [Saunders, 1997]. Discrete Event simulation uses queues to control the flow of elements through a system [Law, 2000]. These simulators are built to help project managers or program directors better understand the interaction of elements, whether they are people, equipment, or dollars, both within and outside of their control, throughout the life cycle of a system. A particularly interesting model is *The Integrated Security Policy Model*, built by Graham Winch and Stephen Sturges of the University of Plymouth in England [Sturges, 1996].

The purpose of this security model was to look at the overall impact of a computer fraud attack on the flow and reconstruction of organizational data, as well as its ensuing impacts on staff, customers, and the bottom line finances. The outstanding characteristic of this model and in this approach is the ability to easily combine many seemingly disparate elements such as dollars, transactions, computers and people all into one model. The key is an analysis of "nth order effects" on the overall health of the organization. This effect is akin to watching a pushed line of dominos. For example the downing of a server could result in the possible loss of records, followed by a loss of customer confidence, then a loss of customers, then loss of staff, and finally the very fall of the organization itself.

In building a MFS, both a user interface and a simulation engine are created by dragging and dropping symbols with built-in behaviors into scenarios. Once built the simulations can be replayed using different input variables. The user simply slides bars or enters new beginning values. The left diagram below portrays six sliding bar inputs, and a single output graph with several output variables displayed. The Security Policy Model allows administrators to play different roles in allocating different percentages of the IT budget to security, and then tossing the dice on possible attacks. One part of the engine in this simulation is depicted in the right image below. This sector contains items such as number of operational PCs and servers and the pressure being placed on the system to get the current workload processed.





A significant benefit to this type of application is the ability to also change the model "on the fly." This would be akin to quickly swapping out one wing on an aircraft for another, and then immediately taking off on a test flight.

These types of simulation models have been used extensively in a number of application areas [Saunders, 1998]. One example in the information technology arena is the *Information Technology Organization Flight Simulator* that was built by Professor Margaret Johnson of Stanford University after foundational work by Tarek Abdel-Hamid [1991]. This simulator allows groups to play different roles in a project-based production of computer code. Another example is one by Clark and Augustine [1980]. Their simulator demonstrated how different levels of information quality might affect a firm's overall performance.

Another interesting simulator, the Synthetic Environments for Advanced Simulations (SEAS) was developed at Purdue. It has been utilized to war game cyber terrorist attacks and other malware incidents [Chaturvedi, 1999]. It is now sold as a commercial product called CyberMBA.

An interesting recent development has been the emergence of the Easel Survivability Simulation from the Software Engineering Institute [Easel, 2001].

> "Easel is a general-purpose modeling/simulation language and tool that is used to predict behavior in a seemingly uncertain world. Easel can be used to simulate systems in which there are large numbers of interacting participants (human or otherwise) that have limited knowledge of the global system properties. Such systems (where the participants in the system have limited visibility) are called unbounded and include the Internet, electric power grids, telephone systems, biological systems, the stock market, and software organizations."

This simulation tool holds promise in that given its basic structure a wide variety of simulation types may be developed under its architecture. To this point we have covered only those types of simulation that utilize technology and provide fairly detailed activity on either the system administrator or computer security manager level. How might we better aid the learning of all participants, especially those who do not have the time to learn about the technical details of computer security? One very open option is to act out scenarios as role players.

Role-playing

In their basic form, these types of simulations utilize no computer-based simulation. They are face to face, actor-oriented. Their purpose is to play out scenarios, more often on a national level, to gain a better understanding of the roles of different organizations and personnel in defending large-scale attacks. Examples include *The Day After … in Cyberspace II* [Anderson, 1997], a Presidents Commission on Critical Infrastructure Protection (PCCIP) Strategic Simulation created by Booz, Allen, & Hamilton [Critical, 1997], a game played annually by Winn Swartou at the InfoWarCon Conference [InfoWarCon, 2001], Cyber War at CSI 27 [Bliss, 2000], and *Dark Winter* [Roberts, 2001]. Although Dark Winter is about BioTerrorism, it still conveys the type of strategic level decision-making and containment skills that would be necessary in a massive Cyber Terrorism event.

The advantage to these types of simulations is the heavy weight upon the human variable in the InfoSec = People + Processes + Technology equation. These exercises require accurate expertise and careful planning to package a simulation that represents the workings of complex relationships either within or among the organizations that may be involved in a cyber attack and defense action. Players would include operations and information management, as well as multiple police, legal, and coordination agencies across many jurisdictional boundaries. Internal and external political factors play a heavy role in these simulations.

Figure 3 - Role Playing Exercise in Action

Summary Comparison

We have now looked at 5 distinct simulation types. The table below provides a synopsis of factors that might be utilized for guidance in which direction a security program manager may wish to take.

	Role Playing	"Canned" Attack/Defend	Packet Wars	Flexible Network Design	Mgmt Flight Simulators
Audience	General	Trained in IT but not security	Network Admins	Researchers	Gen, IT, & Secur. Mgt
Example(s)	Swartou, Christy	CyberProtect ISWS	IOWars, USMAv.AFA	OPNET, Netrule	Ithink, Powersim
Initial $	Low	High- Very High	High	Moderate-High	Moderate
Repeating $	Low	Moderate - updates	High	Low-Moderate	Low-Moderate
Time to build	Hours/ Days	Months/ Years	Weeks/ Months	Days/ Weeks	Weeks/ Months
Time to reset	Instant	Instant	Days	Hours	Instant
Learning curve	Fast	Fast	Moderate	Slow	Fast
Learning effectiveness	Fair	Excellent	Excellent	Good	Good
Level of detail	Poor	Fair	Excellent	Good	Good

Types of Simulations - a comparison

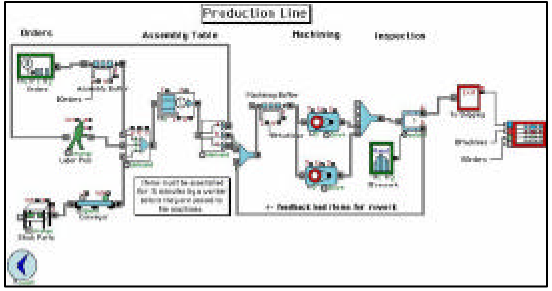
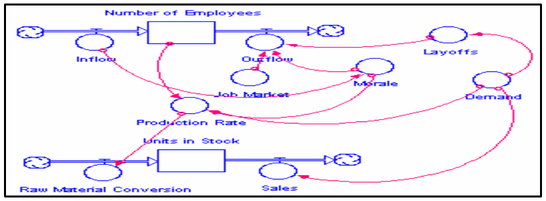
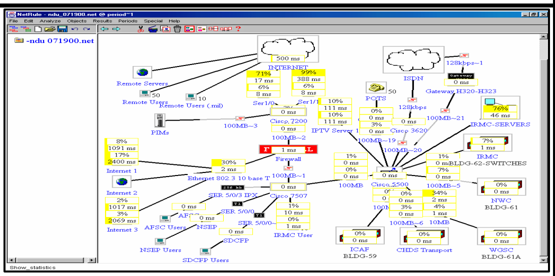
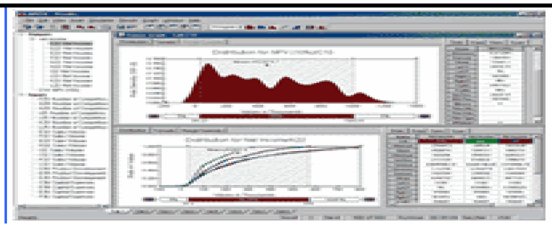
Resources Necessary for Using or Creating Simulations

As stated earlier, it has been estimated that 300 man hours are necessary to build 1 hour of effective multimedia. So while it may be attractive to use simulations, perhaps a larger issue is whether the educator has the sweat equity available to build them. For the educator it is not just the time necessary to build a model, but the time necessary to learn the modeling technology and to build a skill set in modeling. This can mean man-years in time investment. At the same time capturing the essence of a system is just as much art as it is science. Questions such as the following must be considered:

- What are the variables we wish to capture?
- Does the system behavior accurately reflect the real world behavior?
- What level of granularity is necessary to drive home the principles we wish to convey?

The table below provides some guidance for an educator wishing to further explore this tool arena. As in many areas educational discounts are available for those wishing to use the tools available.

Computer Simulation Methodologies & Tools

Method	Characteristics	Representation	Tools/Vendors	Package Cost
Discrete Event Simulation	Queuing, Units moving among service modules, Iconic / Symbolic Representation/ Graphical Interface / Customized animation graphics, Statistical Analysis of Processes, Drag & Drop, Quick turnaround times	 Production Line Orders Assembly Table Machining Inspection	- ProModel, ProModel Corp - Extend, Imaginethat - SimScript, CACI	$1-20K
System Dynamics	Stocks & Flows, Cause & Effect, Concrete & abstract representation, Drag & Drop	 Number of Employees Inflow Outflow Layoffs Morale Job Market Demand Production Rate Units in Stock Raw Material Conversion Sales	- Ithink, HPS, Inc - Powersim, Powersim Corp - Vensim,	~$1K
Sniffer +Design Tool	TCPDump Capture - Feed to Extensive Analysis Tool	 INTERNET ISDN Remote Servers Remote Users Firewall IRMC-SERVERS	- Sniffer, Network Associates - Snort, Snort.org	$50K
Spreadsheet Add-in	Provides multi-period dynamics to spreadsheet cells		- @risk - Crystal Ball - GeneHunter, Ward Systems	<$1K
Custom - Procedural	Fixed Path Heavy Visualization	Procedural Algorithms	- Visual Basic - Authorware	~$1K

Summary

The purpose of this paper has been to present the options and some of the issues with respect to using simulation as a tool for Information Security Education. Modeling is not a perfect science but it is an effective method for visualizing and communicating concepts that are complex and amorphous. Common criticisms with modeling include "garbage in, garbage out", the absence the "right" variables, and the difficulty in modeling human behavior. All of these issues, however may be mitigated by careful planning and properly setting the scope of the learning experience. In this regard simulation should be considered more seriously by the information security community for capturing the essence of the challenges of the field. And to this point a number of simulations have been presented. While the sources of these simulations sprout from considerably disparate genesis, each type presents a distinct benefit to the community. Hopefully this paper has provided an *entrée* into a better understanding of both what is available and what may be possible.

References

Abdel-Hamed, Tarek, and Madnick, Stuart. Software Project Dynamics: An Integrated Approach. Prentice Hall. 1991.

Anderson, Robert H and Hearn, Anthony C. An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After ... in Cyberspace II." Rand Corporation Report MR-797-DARPA. 1997.

Bertsche, D. Crawfords, C. and Macadam, S. Is Simulation Better than Experience. McKinsey Quarterly. Number 1, 1996.

Bliss, Ron. Cyber -War. 27th Computer Security Institute Conference. 2000.

Chaturvedi, Alok and Mehta, Shailendra. Avoiding A "Electronic" Maginot Line: Simulating Information Security Issues for On-Line Banks. CERIAS. Purdue University Research. 1999.

Cohen, Fred. Simulating Cyber Attacks, Defense, and Consequences. March 1999. http://www.all.net/journal/ntb/simulate/simulate.html

Critical Infrastructure Protection Strategic Simulation Report http://www.ciao.gov/PCCIP/StrategicSimulation.pdf. 1997.

Denning, Dorothy E. The Limits of Formal Security Models. NCS Security Award Acceptance Speech. October 18, 1999. http://www.cs.georgetown.edu/~denning/infosec/award.html

Easel Survivability Simulation. http://www.cert.org/easel/

Forio Business Simulations. http://www.forio.com/about.htm

Hill, John M.D. et al. Using an Isolated Network Laboratory to Teach Advanced Networks and Security. Unpublished paper. Contact hillj@cs.tamu.edu. 2000.

Hosmer, Hilary. Visualizing Risks: Icons for Information Attack Scenarios. NISSC Conference, Baltimore MD. 2000.

http://www.saic.com/natsec/model.html

InfoChess Home Page, Aegis Research Corporation. 2001. http://www.aegisresearch.com/info_chess1.htm

Janssen, Will. Explorations in Theoretical Aspects of Information Warfare

JSIMS. http://www.jsims.mil/

Law Averill M. and Kelton W. David. Simulation Modeling and Analysis. Third Edition. McGraw-Hill, 2000.

Letteer, Ray. Information System Security Education, Training, & Awareness for Web Administration – An Integral Part of Defense-in-Depth. SANS Institute Security Reading Room. September 16, 2000. http://www.sans.org/infosecFAQ/legal/infosec_edu.htm

Modeling and Simulation Activities in Support of Information Assurance: Technical Report, IATAC, Defense Technical Information Center, Ft Belvoir, VA. December1, 1997.

Moitra, Soumyo and Konda, Suresh. Managing Survivability of Networked Information Systems. CMU/SEI-2000-TR-020 Technical Report. December 2000.

Moore Andrew P., Ellison Robert J. and Linger Richard C. Attack Modeling for Information Security and Survivability. Technical Note: CMU/SEI-2001-TN-001

Netwars. http://www.disa.mil/D8/netwars/netwars.html

Roberts, Roxanne. "A War Game to Send Chills Down the Spine." The Washington Post. October 23, 2001.

SANS IO Wargames Lecture Series. September, 2001. http://www.incidents.org/Iowargames/soon.htm

Saunders, John. Management Flight Simulators. Info Tech Talk. Spring 1998. http://www.ndu.edu/irmc/newletters/spring98/itt-98-spring.html#C or http://users.erols.com/jsaunders/papers/mfs.htm

Saunders, John. System Dynamics Basics. Info Tech Talk. Spring 1997. http://www.ndu.edu/irmc/newletters/spring97/itt-97-spring.html#Quick or http://users.erols.com/jsaunders/papers/sysdyn.htm

Schrage, Michael. Serious Play: How the Worlds Best Companies Simulate to Innovate HBS Press, Boston, MA 1999.

Shafer, J, et al. The IWAR Range: A Laboratory for Undergraduate Information Assurance Education. Unpublished paper. Contact dd9182@usma.edu. 2000.

Smith, Roger . Simulating Information Warfare Using the HLA Management Object Model

Stackhouse, Brent. Why Do Hackers Have the Advantage? The Problem with a One-Dimensional Security Approach. SANS Institute Security Reading Room. January 25, 2001. http://www.sans.org/infosecFAQ/hackers/hackers_advantage.html

Sturges, Stephen and Winch, Graham. Computer Attack: The Role of Modeling in Developing an Integrated Security Policy. Proceedings of the International System Dynamics Conference, Cambridge, MA. 1966.

Swain, James J. Simulation Software Survey: Power Tools for Visualization and Decision Making. OR/MS Today. February 2001.

Tanner, M., Elsaesser, C. and Whittaker, G. "Security Awareness Training Simulation." Unpublished paper, Mitre Corporation. 2001.

Toorcon Conference. http://www.toorcon.com. 2001.

Trewolla, John. An Inexpensive Personal Security Training Laboratory. SANS Institute Security Reading Room. January 25, 2001. http://www.sans.org/infosecFAQ/start/lab.htm

Tuttle, Dennis. Out with playbooks … in with laptops: Technology transforms the way coaches and players prepare. NFL Insider. December 2000. http://www.nfl.com/insider/december/laptops.html

Waag, Gary L. et al. Modeling and Simulation for Information Assurance: State-of-the-Art Report, IATAC, Defense Technical Information Center, Ft Belvoir, VA. 2001