Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Modeling the Silicon Curtain

One of the challenges that stands before the security community is to make the life of the information security manager more effective and interesting while simultaneously reducing the anxiety associated with responding to information security crises. One clear approach to achieving this goal is to utilize modeling and simulation for education, training, and testing. This paper will present the available range of modeling and simulation capabilities in Information Assurance. It will also establish some principles for e...

Copyright SANS Institute
Author Retains Full Rights

AD

Modeling the Silicon Curtain
Version 2.0 (revised August 13, 2001)
John H. Saunders
October 6, 2001

"When I hear I forget. When I see I remember. When I do, I learn." Confucius

Abstract

One of the challenges that stands before the security community is to make the life of the information security manager more effective and interesting while simultaneously reducing the anxiety associated with responding to information security crises. One clear approach to achieving this goal is to utilize modeling and simulation for education, training, and testing. This paper will present the available range of modeling and simulation capabilities in Information Assurance. It will also establish some principles for extending these capabilities into the community. It will do this by establishing a case for utilizing more simulation in our discipline, reviewing past modeling & simulation efforts within Information security, reviewing the traditional types of modeling and simulation methodologies, addressing capability and experiences in computer modeling within other areas such as telecomm and economics, and providing a framework for future computer based modeling and simulation efforts in Information security.

Introduction

The life of the computer security manager is often one of boredom punctuated by instances of sheer terror. The reasons are obvious. As an overhead cost, the organization wants to keep investment in security to a minimum. So the security manager allocates his budget dollars as best he can, spreading it among defenses such as anti-virus software, firewalls and minimal user training. Then he sits and waits. When the new virus terror hits, he is shaken out of bed to spend 72 hours without sleep answering questions from customers and management about just how the devil got through the "silicon curtain" this time. Promoting a better understanding of the information security environment, quantitatively and qualitatively, statically and dynamically, locally or globally can be effectively achieved through the use of modeling and simulation.

Modeling is the process of capturing the essence, through symbolic representation, of a real world system. *Simulation* is the exercising of a model, i.e. adding dynamics. In simulation, the primary independent variable is time. Most models by nature are not dynamic. For example the OSI 7 layer model is static. But a series of snapshots of this model as bits are stripped from (or added to) a packet moving up (or down) the OSI "stack" provides a simulation that can portray significantly more meaning to the concept of layering.

Modeling and Simulation (M&S) is an effective technique to use during those times when information security threats are not acute. The use of M&S can provide both information security and lay managers a better understanding of their information

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

environment on both on a concrete and abstract level. ***Proactively*** it can be used to identify weaknesses and ***reactively*** it can provide education and training using "what if" scenarios. Ultimately when new threats are introduced the ability of the organization to respond is significantly enhanced.

The Case For Computer Simulation In The Security Arena

"The more you sweat in training, the less you bleed in combat." Navy Seals

Organizations that must fight battles – teams in the NFL, the FBI, the military, all regularly model and simulate/practice their battles. Many of the NFL teams have sophisticated computer models that pit their player's abilities and the team strategies against the other teams. Just ask the head coach of the world champion Baltimore Ravens, Brian Billick [Tuttle, 2000]. He uses computer models extensively.

The FBI also has extensive computer models for envisioning, tracking and simulating complex criminal activity. These dynamic models can include representations of "players" and their contacts with other players, their travel, conversations, and financial transactions. On a more physical basis the FBI has large training sites in Beltsville, Maryland and Quantico, Virginia where all types of police action scenarios are played out daily.

And the U.S. Military forces, when not in actual policing actions or combat spend their entire time in preparation and rehearsal. The U.S. Army's Simulation Training and Instrumentation Command (STRICOM) has an apt phrase, "All but War is Simulation." Over the next eight years this branch of the Army alone will spend $4 billion on simulations. Major simulation efforts in the U.S. Military related to computing and communications include JWARS, NETWARS, and JSIMS[1].

There is evidence that utilizing simulations is actually better than the education provided by real world experiences. At the Institute for Simulation and Training in Orlando Florida, scientists discovered that among participants who were asked to explore a building, those who utilized virtual reality, a branch of simulation, learned much more than those who were given an equal amount of time to physically explore the building. For airline pilots simulators provide scenarios that would be much too risky to duplicate in the "real" world. The FAA gives equal credit to pilots for time spent in a simulator as time flying a real aircraft. Simulations of the interaction of factors in large scale, long-term projects have yielded tens of millions of dollars in savings [Saunders, 1999].

Issues with Level of the Audience Level

To repeat, the challenge then for the security community is to make the life of the information security manager more effective and interesting while simultaneously reducing the anxiety associated with responding to information security crises. This would apply to the other technical and managerial levels as well. Individuals within the

[1] Joint Warfare System , Network Warfare Simulation , Joint Simulation System. See references.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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 have practiced 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 a Intrusion Detection System (IDS) may operate best within a specific data environment. Only through exercise can these capabilities be effectively learned. *It is too late to respond after the crisis has occurred or 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.

M&S 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.

This paper will focus largely on the Education and training aspects, although there is obvious "bleed" into each of the other areas.

Specific Benefits of Simulation

The information security community demonstrates a need for a modeling and simulation capability. The alternatives for gaining an understanding of attacks and defenses of your own system are limited. 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
- 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?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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/administrators, primarily on the local network, or at best on the 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.

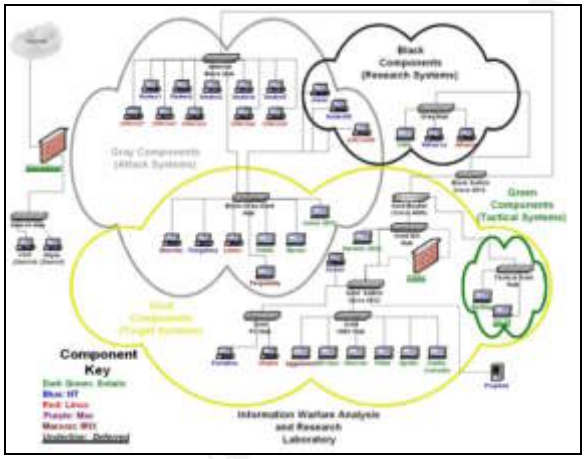


Figure 1 - Academic Security Network at US Military Academy

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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. Earlier this year 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 attempting to scan and attack the weak points in their opponents 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. But the drawbacks are also 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. In the competitions the network must be built from scratch. 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

Professional system administrators and systems application designers 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.

The table below provides a listing of some of the vendors in this market space

Name	Company	Price	Contact	Comments
Cnet	Univ Western Australia	Free	www.cs.uwa.edu.au/cnet/	Good learning tool

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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	Has been 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. The diagram below from the Defense Information System Agency's Modeling and Simulation branch provides a look at the process they utilize for the analysis of networks. This same approach can be utilized for the immediate modeling of availability, but also extended for other analyses such as the spread of viruses.

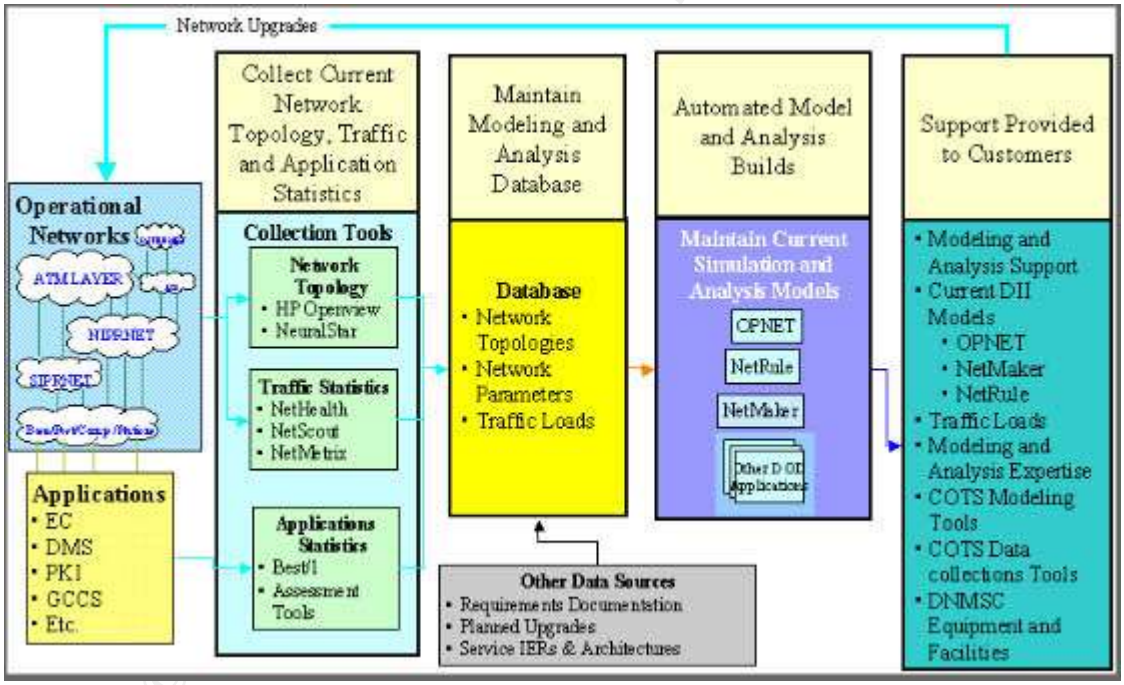


Figure 2 - DISA Network Modeling and Simulation Methodology

Source: DISA D8

There are drawbacks to utilizing Network Modeling and Simulation Packages for the security analyst. They include:

- There is no "built-in" representation of software execution.
- Vendors are now only beginning to focus on memory resident processes.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- 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 solely toward network engineering.

The simulation types we have covered to this point have been aimed at the micro 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? To overcome these resource hurdles, some organizations have focused upon building "ready, out of the box" simulations. The closest approach to Packet Wars and Sniffers +NMS is the “Canned” Package approach.

Canned Attack/Defend Scenarios

These models are typically standalone applications that can be utilized in a game like manner to facilitate learning. These simulations would most often be used by individuals who are trained in IT, but not conversant in the finer points of information security. 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” must be built into the simulation, i.e. the internals of the simulation are not easily modified. 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 attack and defense viewpoint.

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

InfoChess, which is focused on Military Information Operations, stems from a 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.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

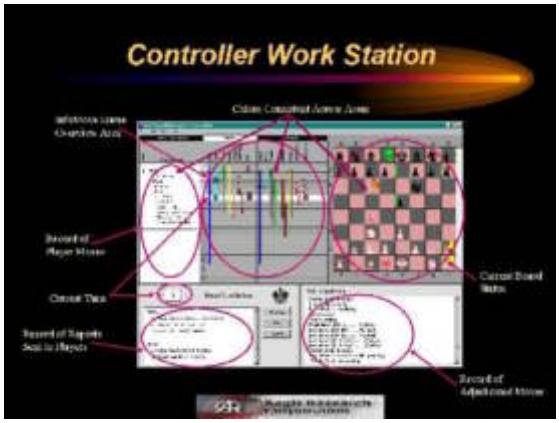


Figure 3 - InfoChess Controller Station

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 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, and therefore receive a final high score. On the other end of the spectrum, he might do a pretty good job in allocating the resources, yet because of numerous attacks, the ending tally would look bad. Even with perfect

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"known" defenses, the enemy may still slip through. The CyberProtect CD is distributed free of charge to qualified government personnel.

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 qualified government personnel from faculty at the IRM College at the National Defense university.

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? There are some interesting alternatives for them.

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]. MFS's 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. An example, The Integrated Security Policy Model, with model sectors pictured below, was built by Graham Winch and Stephen Sturges of the University of Plymouth in England [Winch, 1996].

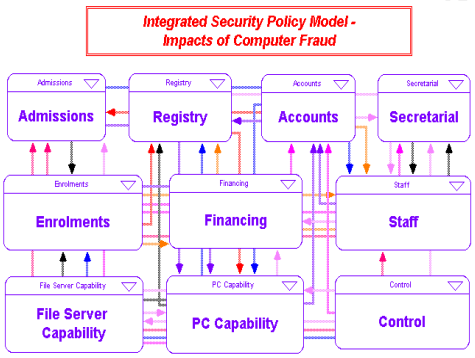
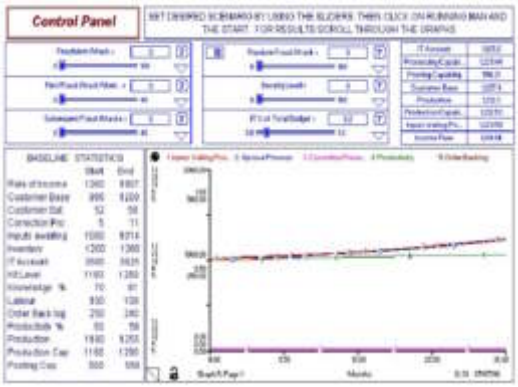


Figure 4 - Integrated Security Management Flight Simulator

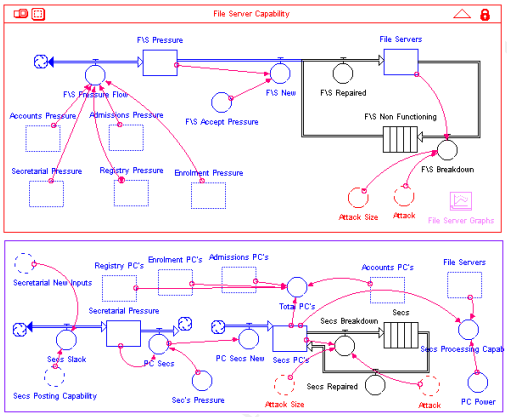
The outstanding characteristic of this model and this approach is the ability to easily combine many seemingly disparate elements into one model. The purpose of this security model was to look at the overall impact of a computer fraud attack on the flow and reconstruction of organizational data, as well as its ensuing impacts on staff, customers, and the bottom line finances. The key is an analysis of "n^{th} order effects" on the overall health of the organization. The nth order effect is akin to 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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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 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 below. This part 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 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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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 in this simulation area is 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 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

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], and a game that has be played by Winn Swartou at the InfoWarCon Conference [InfoWarCon, 2001].

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.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Figure 5 - 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

Summary

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

As in many other areas where there is chaos in growth, for the security arena to progress there is a need for the community to come together on representational formalisms. Such agreements exist in the some areas of the simulation realm, such as the DEVS Formalism, the Systems Dynamics method, and in State Space/Petri Net modeling [Moitra, 2000]. But conceptual agreement on a model as a basis for portraying a comprehensive, provable, understanding of security arena is still very much in debate [Denning, 1999]. Nonetheless, as a base, security professionals would likely benefit from a better understanding of basic concepts in modeling such as levels of abstraction, logical versus physical entities, objects attributes, and scripting.

The purpose of this paper has not been to examine all the issues with using modeling and simulation as a tool. Some universal criticisms of modeling include "garbage in, garbage out", absence the "right" variables, and the difficulty in modeling human behavior. Modeling is not a perfect science. But it is an effective method for visualizing and communicating concepts that are complex and changing. It should be considered more seriously by the information security community for capturing the essence of the challenges of the field. 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.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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/

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.

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

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

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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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.

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.

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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**