Military Academy Attack/Defense Network

Curt A. Carver, *Member IEEE,* John R. Surdu, *Member IEEE,* John M.D. Hill, *Member IEEE,*
Daniel Ragsdale, *Member IEEE,* Scott D. Lathrop, Timothy Presby, *Member IEEE*

Abstract – One can argue that Information Assurance education is vitally important. It is often impractical to allow students to experiment with real networks. A simulation-based tool is needed to supplement classroom instruction. This paper introduces the Military Academy Attack/Defense Network (MAADNET) that allows users to explore interrelationships between people, procedures, hardware, software, and data and how each of these factors impact on network design and security. MAADNET uses a client-server architecture in which the user builds and tests a network design on the client side and later submits the planned network to the server. The server simulates various events and grades the network based on "hard" metrics like message latency, percent down time, etc. The network is also graded on "soft" metrics like how well confidentiality, integrity, and availability were maintained during simulated attacks.

Key Words: Information Assurance, Network Simulation, Education

I. Introduction

Computer networks are ubiquitous, but people who know how to design and build them are rare commodities. It is rare to find a computer science program in any college that does not offer a computer networks course; academia has recognized the importance of education in this area. Often this education is focused on network protocols and theory with little emphasis on the hands-on application that system administrators face every day. While both forms of computer network education are equally important, the tool described in this paper addresses the more hands-on aspects of network design.

Information Assurance (IA) education and training in today's world is even more important. Several incidents in the past few years, such as the Code Red worm, ILUVYOU virus, and defacement of the White House Web page, emphasize the requirement to train and educate users and administrators of information systems. IA is more than just applying technology to secure an information system. To provide assured information an organization must have personnel who are properly trained in the employment of that technology. In many organizations this human element of maintaining security is overlooked.

The IA model provides an excellent framework for assessing information assurance concepts, as shown in Figure 1. The model describes four dimensions: (1) information states, (2) information services, (3) information security measures and countermeasures, and (4) time [1]. Looking more closely at security measures and counter measures, it is apparent that policies and procedures, technology, and people together have a synergistic effect on the security of an information system. Of these three elements, people are the key component. It is people, relying on the knowledge that they have acquired through IA education opportunities, who must develop the policies and procedures that define what information is valuable, who is responsible for protecting that information, and the controls system administrators and users must implement in order to safeguard the information [2]. In addition, people must build, install, configure, and maintain the technical aspects of information systems such as applications, operating systems, intrusion detection and response systems, vulnerability assessment systems, integrity maintenance systems, firewalls, and forensic tools. Such tools attempt to prevent an attack on an information system, detect intrusions, and if necessary, recover and restore lost information. If technology is implemented improperly or is used without the correct policies and procedures to support it, technology can actually *reduce* the overall security of an information system. Finally, it is people who must hire, retain, and sometimes fire other people who use and maintain these information systems. Without education and training in such matters, information security measures are nearly worthless.

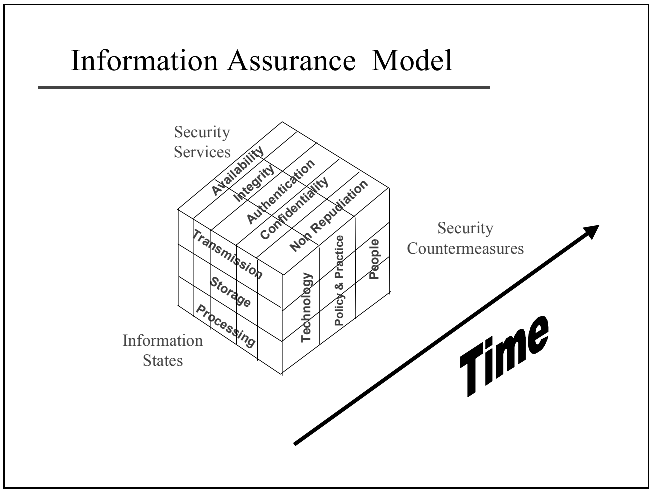


Figure 1: Information Assurance Model

The United States Military Academy (USMA) offers two IA courses for cadets. To enhance the quality of the IA education experience for students, the Department of Electrical Engineering and Computer Science has supplemented conventional instruction methods with two

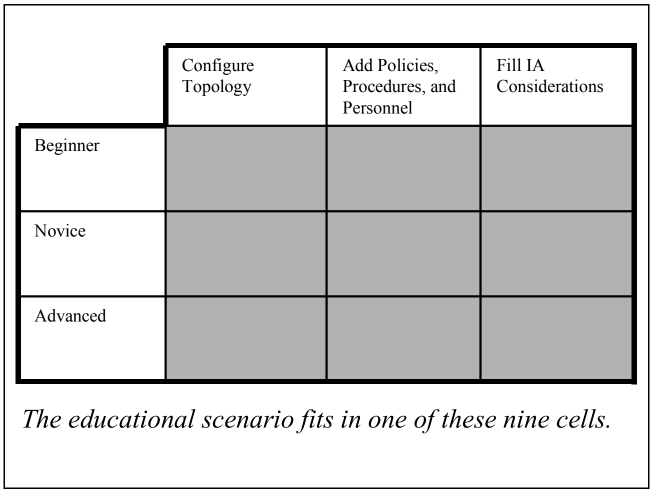
Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY 10996, {curt-carver | john-surdu | john-hill | dan-ragsdale | scott.lathrop | tim-presby} @usma.edu

new innovations. First, a sophisticated information warfare laboratory was built. This isolated network of computers and communications components provides an environment that facilitates active learning and provides maximum opportunity for hands-on experience [3]. In addition, students participate in a large-scale, inter-service-academy competition, the Cyber Defense Exercise, in which they design, implement, configure, and secure a network of computers. These networks are subjected to cyber attacks from personnel on a National Security Agency-led "red team." The winner of the competition is the school that is determined to have provided the most viable network defense.

These two components of the IA education program at West Point provide for a much richer experience for students than mere classroom instruction. Unfortunately, both require significant investments in terms of hardware, software, and human resources to build and maintain the physical networks of computers and communication components. This is not a unique problem. Due to the increasing importance of IA education, many colleges and universities are investing heavily in the construction of information security laboratories. What is currently lacking in IA education programs is a tool or model that can be used by students to assess the quality of their information system design choices prior to (or instead of) a physical implementation.

A network analysis tool (for either education or decision support) that has a simulation component has many benefits. The U.S. military learned long ago that it is impractical, from a standpoint of both time and money, to send soldiers to the field to train on their equipment without prior training using less-expensive simulations and simulators. So too is it impractical to let students build large networks, test the performance of those networks, and learn from their mistakes. Simulations also allow the proposed network to be tested under a larger variety of conditions and attacks than would be feasible with a real network. There may also be a number of attacks that are too dangerous to perform on the real system. [4]

A simulation model that one could leverage as an instructional tool and/or a design tool would fill such a gap. For example, using an IA simulation, a student or network administrator could plan and design an information system that is secured through polices and technology. That individual, prior to actually building the network, could then assess the design using a tool like MAADNET, described in this paper. This methodology would not only educate the person, but also save considerable time and effort during the actual implementation of the computer network. Such a simulation forces the student to both think of IA concepts and actually apply those concepts in the design of an information technology system. Unfortunately such a tool does not exist.



	Configure Topology	Add Policies, Procedures, and Personnel	Fill IA Considerations
Beginner			
Novice			
Advanced			

The educational scenario fits in one of these nine cells.

Figure 2: Possible Configurations of the Simulation

II. Related Work

Many different networking design and simulation packages already exist, such as OPNET, NetworkCracker, NetRule 2.3, EcoPredictor 3.0, NetCracker, and Opnet DecisionGuru 6.0 [5-9]. These tools allow for the effective design and deployment of networks and network technologies and the simulation of network traffic against the network design. They provide a wide range of capabilities and often have a steep learning curve associated with them. Saunders described several features of traditional network simulations that make them unsuitable as educational tools, among them an engineer-oriented user interface and no representation of "soft" factors, such as social engineering and level of user training [4]. Illustrative of these packages is OPNET. The OPNET product suite consists of a set of predictive modeling tools and a simulation package. The OPNET suite allows users to diagnose network and application performance problems and predict the impact of network changes. The scope of this product allows users to model and simulate network entities at many different levels, from the process model level using C programming language code through global network models using commercially available devices [5].

These tools were developed to support decisions regarding network architecture and to test new protocols. Often the level of detail involved in these simulations makes their use difficult. It is reasonable to desire a high fidelity, lower-detail model for typical network design applications. (The reader should not confuse fidelity with detail. Fidelity is a measure of the model's ability to predict the performance of the real system. Detail is a measure of the number of parameters used in the simulation. While often related, fidelity and detail are independent measures.)

While these tools are appropriate for business network design, they are poorly suited for pedagogical purposes. The steep learning curve associated with these tools precludes mastery in a single semester. The packages assume mastery of the networking concepts MAADNET proposes to address. There is no capability for simulating information assurance attacks or for simulating the action-counteraction interaction inherent in information assurance attacks. There is no capability for readily comparing the different network designs. Finally, the cost of these tools prohibits their widespread use for educational purposes.

Other efforts have been directed at increasing a user's understanding of communication networks or information assurance such as Network Tutor, CyberSecurity, or the Seminar Wargame Interactive Exercise (SWIE) [10-12]. Network Tutor is illustrative of these efforts. Developed by students as part of an educational technology course at the Georgia Institute of Technology, Network Tutor uses goal-based scenarios to increase a learner's skill set. For Network Tutor these skills include evaluating user needs, network design skills, and network troubleshooting. In addition to a goal-based learning approach, network tutor includes a cognitive apprentice approach based upon reciprocal learning [10].

While this project uses many well-developed pedagogical methodologies to promote network learning, it lacks the range of functionality and simulation capabilities required for MAADNET. There is no capability for simulating the action-counteraction interaction inherent in information assurance attacks. There is no capability for readily comparing the different network designs. Based on these limitations, MAADNET is being explored.

III. Methodology

The Military Academy Attack/Defense Network (MAADNET) is a simulation-based pedagogical tool that allows the user to explore network construction, information systems, and information assurance. Users construct networks, impose policies, and hire administrators. (While many of the underlying components of MAADNET have been prototyped, a MAADNET prototype does not yet exist.) After constructing a network, the user will run a series of scenarios against the network and watch as the network fails or succeeds based on network load or security attacks. MAADNET will allow the user to explore the interrelationships between people, procedures, hardware, software, and data and how each of these factors impacts on network design and security. It will supplement in-class presentations, experimentation in the information assurance laboratory, and experiences in the Cyber Defense Exercise by allowing cadets to virtually answer the question, “What if?”

A. Web Based Architecture

The short-term vision for MAADNET is a tool to supplement classroom instruction in computer networks and information assurance. The longer-term goal of MAADNET is to facilitate a web-based competition in which competitors from across the country submit their network and security plans to the server. The server will simulate this plan through some scenario (such as a series of outages or hacks) and evaluates the plan, giving it a score. To facilitate this long-term vision, the overall architecture of MAADNET is client-server. The server will contain the simulation engine, the attack scenario, and the evaluation mechanism. The client will contain the (defensive) scenario generator, network builder, and simulation viewer. In order to maintain platform independence, the technology that will facilitate this client-server architecture will be either signed Java applets [13] through a Web browser or a relatively new technology, called Java WebStart [14], which allows the remote invocation of Java applications vice applets.

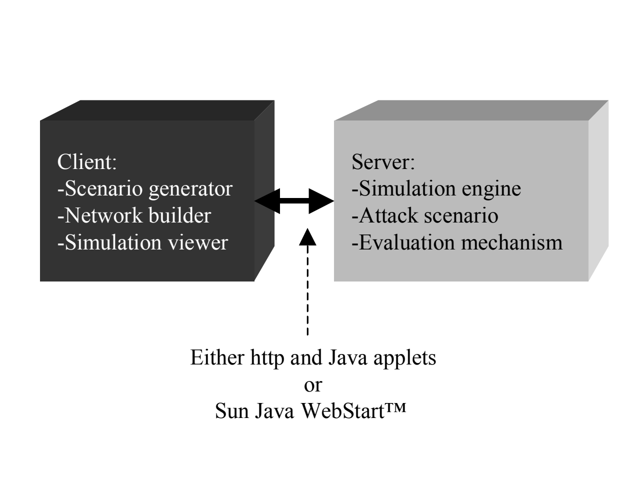


Figure 3: Client Server Architecture of MAADNET

The simulation engine will be located on the server so that the engine cannot be analyzed to determine the best strategy. Similarly, the attack scenario will be located on the server so that the users cannot merely optimize their system for one scenario. The client machines will permit users to build network topologies and emplace information assurance tools. The user's (network and defense) scenario will be stored locally on the client machine until the user submits it for evaluation.

The advantage of the applet methodology, regardless of the language used to write the applets, is that anyone with a reasonably recent Web browser has access to the system without downloading any special software. In general the use of applets also permits a more sophisticated interface than the use of scripts. Since the simulation prototype on which MAADNET will be based was written in Java, it seemed natural (but not essential) to use Java for the user interface as well.

In general, Java applets are not allowed to access local resources, such as the file system. Signed applets use a public/private key encryption mechanism to certify that the applet has come from a trusted source. These trusted applets can then be granted limited access to local resources. Applications are not hampered by these requirements. Sun's Java WebStart technology allows a user to download *applications*, vice applets, through a Web browser and run them locally. The other advantage of WebStart is that whenever a user tries to launch the application, WebStart first checks the date of its cached copy of the application against the date of the application at its source. If there is a newer version of the application, it is downloaded and then run; otherwise, the cached version is launched.

B. Server

1) Simulation engine

As the purpose of this project is to provide a tool for education and mid-level decision-making, the MAADNET simulation engine is not concerned about the flow of individual packets or the performance of various communications protocols. MAADNET concentrates at a higher level. Lower-level network management will be accounted for as background utilization and will merely decrease available bandwidth. Entities are defined as those aspects of the system that can generate messages. Entities can be hardware, such as routers, workstations, switches, wireless access points, etc. Users are subsumed by their workstations, and the users' profiles affect the traffic generated by those workstations.

In order to generate messages, entities have one or more traffic generators attached to them. Traffic generators generate specific types of messages to specific types of entities. For instance, a traffic generator generates Email messages to the Email server at a given rate. The rate at which messages are generated and the size of the messages is determined in one of three ways: a fixed rate, a standard family of probability distribution (e.g., normal distribution, exponential distribution, etc.), or an empirical distribution.

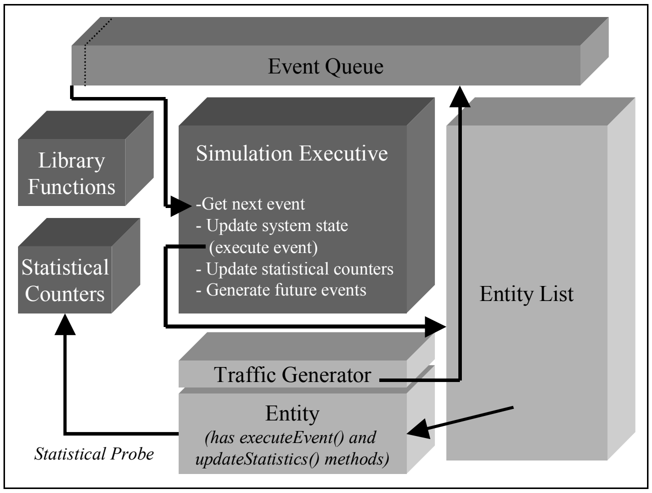


Figure 4: Basic Design of the Simulation Engine

Entities also can generate events based on their Mean Time Between Failures (MTBF). Whether or not the full IA aspects of the simulation are being simulated, equipment fails. If a node has failed, messages bound for those nodes cannot be delivered. The entity representing the delivering node must handle the inability to deliver the message accurately (e.g., dropping messages, buffering messages, etc.). Entities are also rated on their Mean Time to Repair (MTTR). This MTTR may later be modified by the proficiency of the assigned system administrators.

As shown in Figure 4, each entity has a series of executeEvent(…) methods, one for each event type that the entity can receive. The simulation executive pops the next event off the event queue, identifies the entity that is supposed to execute that event, and calls that entity's executeEvent(…) method, with the event as a parameter. While executing an event, the entity may generate future events. These events are then added to the event queue, which places it in correct location chronologically. While executing events, entities also update the simulation's statistical counters through the statistical probes that have registered with the Entity.

When MAADNET is being used to teach information assurance topics, probabilities of attacks succeeding must be determined. The probability of an attack succeeding is based on the type of attack and the skill of the attacker. It is also based on the network topology, the skills of the system administrator(s), level of user training, the types of defenses that have been put in place, etc. (These "soft" attributes are equally important even if IA is not part of the scenario.) Initially these attack probabilities will be determined in a subjective manner, through interviews with experts. Developing good models of these attack-defense relationships remains an open research issue.

The prototype network simulation that will form the basis for the MAADNET simulation engine, dozens of nodes have been simulated with several traffic generators at each. The runtime performance with a network of low complexity is very fast. This prototype has not yet been tested with hundreds of nodes.

The coarse level of detail of MAADNET will nonetheless provide the appropriate level of fidelity for a computer networks class. It will also provide the appropriate fidelity for an information assurance course. Attacking nodes can be added to the simulation. These nodes generate attacks (also represented as messages flowing from attacking workstations) that may cause events to be generated and added to the event queue.

2) Evaluation mechanism

Since this is both a teaching tool and a decision support tool, metrics must be identified to help rate the goodness of the network (and information assurance) plan. Metrics used in MAADNET include rating the overall message latency, link percent down time, and node percent down time. These metrics are easily collected and computed, and they are combined into an aggregate measure, called productivity. Cost to build, maintain, and repair the network are also easily computed.

MAADNET will also evaluate performance against the confidentiality, integrity, and availability attributes shown in Figure 1. Use of MAADNET will be scenario driven. The scenario might indicate, for instance, that in the user's organization confidentiality is vitally important. A successful attack against availability, then, would have less impact on the user's evaluation than would a successful attack against confidentiality.

Eventually, the user will be given a score, between zero and one hundred, where zero is the worst. This score could be used for general feedback to the user, for grading purposes in a networks or information assurance course, or as the basis for determining the winner of a competition.

It is important to note that there are no known, implementable models that combine the "hard" and "soft" aspects of information assurance. Information assurance experts will provide initial face validation of the MAADNET evaluation mechanism. Better validation of the evaluation mechanism is an open research issue, which the West Point Information Technology and Operations Center intends to explore.

C. Client:

Development and implementation of the desired network will occur on the client side of the system. To accommodate a variety of purposes, the MAADNET client will operate at several levels, as indicated in Figure 2. The user will receive a scenario at the appropriate level from the server and then configures a solution. Once the solution is configured, the client will provide some feedback. When the user is satisfied with the configured solution, the solution will be submitted to the server, where it will undergo a simulation as discussed in the previous section.

The client software will provide several layers of operation, tied to the desired outcome from using the software. At the lowest level, users will merely configure the hardware and gather feedback on the costs associated with that configuration and whether there are any communications bottlenecks. At intermediate levels, the addition of services and applications, as well as the effects of well- or poorly-trained systems administrators and users will be included. At the highest levels, intrusion detection and response mechanisms will be incorporated and may be tested. This multi-level approach enables beginners to understand the workings of a network, more experienced users to explore issues of what the network supports, and advanced users to address information assurance issues.

The server will provide the client with a scenario appropriate to the levels described above. The scenario includes a list, and associated data, of the equipment available for selection by the user. This includes network devices, types of connections, workstations, servers, and any other appropriate equipment. A description of the physical facilities in which the network will be configured is included in the scenario. In some scenarios, financial constraints will be imposed. At intermediate levels, some internal services (e.g., mail, etc.) and external services (e.g., web servers, etc.) may be required, as well as the capability to support certain business activities (e.g., desktop publishing, word processing, CAD/CAM, etc.). Also, the mechanism for connecting to the Internet may be specified. At the highest levels, hardware and software may be available to address information security issues. Finally the scenario will also include an indication of what aspects of confidentiality, integrity, and availability are most important to the organization.

Once the user has the scenario in hand, the client software allows construction of a network. The user selects equipment, connects it together, and populates the network with the appropriate services and applications. Administration and support personnel, along with their associated costs, can be "hired" to manage the system. The connection to the Internet can be placed behind a firewall, or security software may be applied to servers and workstations.

One of the purposes of the client software is to provide local feedback to the user. This feedback can be as detailed as what networking components can be connected to others. Perhaps the clearest feedback is the running cost of "purchasing" equipment and support personnel. Other feedback can include an assessment of bandwidth bottlenecks for the current configuration and scenario.

IV. Summary and Conclusions

MAADNET is designed to supplement classroom instruction by allowing students to experiment with the interrelationships between people, procedures, hardware, software, and data and how each of these factors impact on network design and security. MAADNET's most significant advantages over existing simulation tools are its degree of interactivity and its incorporation of "soft" metrics.

The IA courses at USMA have a significant hands-on component. Just as simulation/simulator training helps prepare soldiers and pilots for operations with real equipment, MAADNET will help prepare students for their hands-on exercises. This will accelerate learning and enhance the level of expertise of students who have taken these courses.

Currently, early proof-of-concept prototypes have been built. Detailed design is ongoing. Code writing is scheduled to begin in July, and a working systems is scheduled for December 2002 to be used in the information assurance course in the Spring of 2003.

V. References

[1] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A Model for Information Assurance: An Integrated Approach," in *Proc. 2001 IEEE Information Assurance Workshop*, West Point, NY, 2001, pp. 306 - 310.

[2] S. Garfinkel and G. Spafford, *Practical UNIX and Internet Security, 2nd. ed.* Sebastopol, CA: O'Reilly & Associates, Inc., 1996.

[3] H. Schafer, D. J. Ragsdale, J. R. Surdu, and C. A. Carver, "The IWAR Range: A Laboratory for Undergraduate Information Assurance Education," *The Journal of Computing in Small Colleges*, vol. 16, pp. 223-232, 1 November 2001.

[4] J. H. Saunders, "Simulation Approachs in Information Security Education," in *Proc. 6th National Colloquium for Information System Security Education*, Redmond, WA, 2002, pp. TBD.

[5] OPNET Technologies, "MIL3 - Third Millenium Technologies, OPNET," at http://www.mil3.com/, February 2002.

[6] B. Boardman, "Making Sense of Network Chaos," at http://www.networkcomputing.com/shared/printArticle?article=nc/1107/1107f2full.html&pub=nwc, February 2002.

[7] S. D. Post, "Network Planning with a Performance Prediction Tool," *International Journal of Network Management*, vol. 9, pp. 167 - 1731999.

[8] Compuware Corporation, "Predictor," at http://www.compuware.com/products/vantage/predictor/, February 2002.

[9] NetCracker Technology, "NetCracker," at http://www.netcracker.com/, February 2002.

[10] Georgia Institute of Technology, "Network Tutor," at http://swiki.cc.gatech.edu:8080/edtech/431, February 2002.

[11] Concurrent Technologies, "Information Security Wargaming System: Seminar Wargame Interactive Exercise," at CD ROM, February 2001.

[12] C. M. U. Entertainment Technology Center, "CyberSecurity," at http://www.etc.cmu.edu/projects/cybersecurity/objective.html, February 2002.

[13] Sun Microsystems, "Signed Applets," at http://java.sun.com/products/jdk/1.1/docs/guide/security/, February 2002.

[14] Sun Microsystems, "Java WebStart," at http://java.sun.com/products/javawebstart/faq.html, February 2002.