MAADNET: Toward a Web-Distributed Tool for Teaching Networks and Information Assurance

John M. D. Hill, John R. Surdu, Scott Lathrop, Gregory Conti, and Curtis A. Carver, Jr.
Department of Electrical Engineering and Computer Science
Information Technology and Operations Center
United States Military Academy
United States of America
[John.Hill | John.Surdu | Scott.Lathrop | Gregory.Conti | Curtis.Carver].usma.edu

Abstract: There are rarely enough time, laboratory, or equipment resources available for students to explore network construction, provision of services, demand analysis, and information assurance issues. Students need a software tool in which they can rapidly construct networks to satisfy particular scenarios and get rapid feedback. The ability to represent defensive preparations and attacker behaviors raises awareness in the information assurance arena. Making the tool web-deliverable enables a new level of outreach to potential students of networking and information assurance. Faculty and research scientists at the United States Military Academy are developing the Military Academy Attack/Defense Network (MAADNET) to provide the network construction and evaluation tool, including the ability to model attack and defense, and to create a web-based competition format to reach out to prospective students at every level of expertise.

Background and Motivation

Teaching people how to design, build, and evaluate networks, whether for education and training or for industry, usually requires a significant investment in time, equipment, and other resources. Teaching them the specifics of installing and operating services (e-mail, web, file, etc.) and then generating realistic demands against those services is even harder. The desire to inculcate an awareness of information assurance concerns makes it even more complex and resource intensive. Many institutions do not have the laboratory facilities, computer/networking equipment, and the student and faculty time to allow thorough exploration of these areas. Even with great resources, students can't take the laboratory hardware and software with them to practice network configuration and evaluation on their own. This also places practical limits on the ability to reach out to potential students. A web-delivered software tool is sorely needed that allows students and practitioners to virtually construct a range of simple to complex networks, install services, place demands on their configuration, secure it, and evaluate the results.

The Military Academy Attack/Defense Network (MAADNET) is a multi-phase project addressing the problems of time, resources, and inability to reach out. The first phase is development of MAADNET NetBuilder to provide network construction, communication modeling, service and demand modeling, and an underlying simulation to support visualization and evaluation. The second phase will develop MAADNET Competitor to incorporate the modeling of attack behaviors and defense capabilities. The third phase will package MAADNET NetBuilder and MAADNET Competitor for web delivery beyond the classroom. This work is ongoing, with a prototype developed for the network construction, traffic modeling and simulation, and early efforts on device and demand modeling (MAADNET NetBuilder) and attack and defense modeling underway. The contributions of the MAADNET project will include an easy-to-use network construction interface, a less-detail oriented traffic model, a service and demand focus to network modeling, the ability to appropriately portray attacks and defenses over time, and a new way to reach out to potential students. The results of this research should be useful to others interested in networking and information assurance, particularly training and education.

Related Work

OpNet Modeler, a "state of the art modeling and simulation environment that accelerates R&D for engineers designing network equipment, communication protocols, and systems" (MIL3 2002) and similar very sophisticated simulations are available for the construction and evaluation of network hardware configurations, the transmission of packets, and the use of protocols. They are useful for student instruction, but have a fairly large

learning curve, are too detailed for the novice student, and typically don't consider the range of issues that arise in information assurance instruction.

The CyberProtect application is an "interactive computer network defensive exercise … intended to familiarize players with information systems security terminology, concepts, and policy." (Uiterwijk 1999) This product doesn't delve quite as deep as MAADNET intends, however, it addresses services and demands and plays out attack and defense over time.

SimSecurity is a project at the Naval Postgraduate School that will "create a distance learning information assurance [IA] lab … packaged as an interactive game" in which "player may perform various roles involved in IA." (VanPutte 2001) This product is based on the idea that if city management can be made enjoyable in SimCity™ (a registered trademark of Electronic Arts), then information assurance can be made enjoyable in an interactive gaming experience, too. It includes attack and defense modeling and is designed for web-deliverable scenarios, but doesn't delve as deep and doesn't (currently) support external competition.

The West Point Bridge Design project (Ressler 2003) is an example of a web-delivered, web-based competition in which students from around the country (and beyond!) download the bridge design software, developed bridge designs, and submit the designs for evaluation. The design that best satisfies the multiple criteria (cost, load capacity, etc.) in the scenario is declared the winner. This contest is exactly the type of outreach that MAADNET is striving for.

Building the Foundation

MAADNET NetBuilder serves two purposes for the MAADNET project. The first is to let instructors provide an instructional software tool, prepare and distribute scenarios, and let the students develop solutions with the tool. This includes visualization of communication flows, provision of services and meeting of demands, and the use of simulation to aid in evaluation. The second purpose is to serve as the foundation for an information assurance education tool that focuses on awareness of defensive techniques and attacker methods. Ultimately, it will support the web-distributed competition concept.

Network Construction and Evaluation

When building a network simulator, the designers must determine the desired balance between the granularity required in building a realistic network and the details involved in representation of information processing, storage, and transportation. MAADNET NetBuilder is an attempt to find the appropriate balance for use as an educational tool for students, faculty, managers, and administrators of information systems. To accomplish this, a layered design is used that simplifies construction of the system and eases future expansion (one of the prime development considerations, because it is the foundation of the entire project).

Once the students receive the instructor-defined scenario and start building a solution, the system provides immediate feedback as to costs and other factors. The underlying simulation takes the information flows generated by demands on services and provides visualizations of bandwidth saturation and other bottlenecks. The development of applications for network construction, including visualization of results and an eye to the long-term goal of web-based delivery and competition, takes advantage of modern interface and visualization techniques to enable rapid construction and evaluation.

The design allows users to rapidly construct a networked system using aggregations representing standard underlying TCP/IP protocols and standard system security tools (such as firewalls, intrusion detection systems, and vulnerability scanners), without having to worry about the intricacies of what happens at the physical, data link, and networking link layers of the OSI reference model. If the devices can connect, the user is allowed to connect them. If traffic can flow, an aggregation model represents the flow. Scenarios (defined in XML) describe a physical space, the available devices, links, services, and support personnel, and the demands (associated with users) that will be placed on the system. They also define conditions that must be satisfied (availability of mail services, etc.). An important part of the scenario (particularly in the competition aspect of MAADNET) is the definition of costs and other trackable attributes, and the scoring criteria based on those attributes.

Instructors define scenarios to teach or reinforce particular concepts (saturation, for example). The student then designs and deploys the network, emplaces services, and determines policy and procedures. Within the constraints of an initial budget, the user can choose (buy) the hardware to meet the requirements, choose (buy) software tools, and select (hire) the people to administer the system. The configured system can then be subjected to

a series of simulated operations. As MAADNET becomes more sophisticated, levels of user network and IA awareness will be represented, as well as defensive mechanisms and attacks from a spectrum of attackers to include enthusiastic script kiddies to cyber terrorists.

The user interface provides visual network construction, with devices, services, demands, etc., dragged off of selection bars generated from the scenario. A foundation holds rooms that serve as the drop point for device placement, and links are established with drag gestures from one device to another. If linking rules are not satisfied, the drag is not allowed to succeed. Services are set up by simply dropping them on a compatible device. Demands are established by placing people (with their associated demand profile) on a compatible device (usually a workstation). A control panel starts, pauses, rewinds, and stops the simulation. The display panel provides visual feedback on bandwidth utilization, bottleneck identification, costs, and other attributes. The visual drag and drop interface and controls enable rapid configuration and re-configuration and provide immediate feedback, allowing the user to rapidly get the answer to "what-if" questions.

Traffic Modeling and Simulation

The foundation of the layer system is a classic discrete event simulation (DES) architecture. The simulation executive registers entities (simulation participants) and processes requests from those entities to schedule events (such as message arrival times at a device). The events are maintained in temporal order in an event queue. A clock is run in various multiples of real time. At the appropriate time, the executive removes each event from the queue, then notifies the scheduling entity that the event has occurred and must be executed. In the process of executing events, other events may be scheduled. For instance, a traffic generator might generate a message and then schedule the next message-generation event.

With the configurable parameters for representing demands, one can richly define different types of users in an organization, including admin staff, engineers, web developers, programmers, etc. When users are added to the system, their messages generators are added as simulation participants. When a message generation event is pulled from the event queue, it points to a particular traffic generator and calls a method in the traffic generator to create a new message. Generating a message involves determination of the path through the system from the sender to the receiver(s). Once the messages are created the traffic generator schedules two more events: a message arrival event at the first hop on the path and a new message-generation event.

Other types of events are possible, such as equipment-failure events and equipment-repair events. The various workstations, routers, switches, servers, hubs, and other hardware items all have probabilities distributions that define their mean time between failures (MTBF) and mean time to repair (MTTR). The quality and quantity of system administrators may affect both. When the simulation is initialized, each piece of hardware determines stochastically when it will fail and schedules a hardware failure event. When the event is executed, the MTTR is used to schedule a hardware-repair event.

The Communications Layer is the interface that passes generated traffic from the underlying simulation up to the device and link layer. The traffic does not represent packets, and is not managed with packet-level protocols. Instead, demands in the Service and Demand layer cause traffic generators in the Communications Layer to send messages (including bandwidth requirements and other attributes, such as priorities). This aggregation is sufficient to determine bandwidth utilization and to capture statistics for feedback and analysis.

A device is any hardware that participates in the network. This includes computers, routers, network interface cards, etc. A link is any means of conveying traffic between devices. This includes unshielded twisted pair wire, coaxial cables, and even wireless links. Devices and links have defined capabilities, including max bandwidth, number and types of ports, etc. Devices and links are modeled in an object hierarchy that, among other advantages, allows for easy addition of new device or link types.

When the student runs the system, the demands cause message traffic to start flowing. The messages are scheduled into the simulation, with arrival times at devices based on their bandwidth requirement versus the bandwidth available. The interface provides visual feedback of bandwidth bottlenecks, and a score based on criteria defined in the scenario. With this feedback, the user reconfigures the network to improve performance.

Service and Demand Modeling

Once the hardware of the network has been set up and the links established the user must configure the services provided over the network in support of demands specified in the given scenario. MAADNET NetBuilder has models for several kinds of common services, such as file, mail, and web services. As other services are

required, the model can be extended. Services placed on compatible devices respond to demand traffic by producing their own traffic, thereby placing a communication load on the system. The services file specifies the list of services that must be provided to the users. Note that in the case of services, this file identifies the class associated with the implementation of that service within the simulation, making it easy to create a new Webserver subclass.

Demands are associated with people (stick-figure icons) in the system, and include the loads they place on mail, file, web, and other services. Part of the defined scenario is a collection of such people. Associated with each person are a number of traffic generators that generate different types of messages at defined intervals. These intervals can be constant or generated from one of the common families of probability distributions. Users have traffic generators for web access, database access, access to file servers, CPU usage, and Email. Email is further divided into three categories: Email to a single user within the organization, Email to all users within the organization, and Email to the Internet.

The student must provide sufficient services for said demands, and ensure there is enough computing power and bandwidth to support them. This involves making decisions about purchasing hardware and services and in how to configure the network. Placement of people in the system is now a significant issue as well because the demands they create have different impacts depending on which part of the system they are associated with.

Future Work

With MAADNET NetBuilder providing the network construction / simulation / evaluation foundation, the next steps are to incorporate attack and defense modeling, develop the web delivery mechanism, and implement the web-based competition. The specifics of attack and defense modeling in MAADNET are available in (Lathrop, Hill et al. 2003). The ultimate goal of the MAADNET project is to provide a web delivered networking and information assurance competition. Although the mechanics of providing the software and the scenarios has not been decided, Java WebStart (Sun Microsystems 2002) is a leading contender.

Conclusions

MAADNET NetBuilder is designed to be a very valuable tool for instruction in networking and information assurance. The most valuable conclusions come out of student experiences with the NetBuilder prototype. The improvements based on the assessment of those experiences will serve to improve not only NetBuilder, but also the entire MAADNET system that will be built upon it.

The MAADNET system will provide several significant advantages over traditional networking and information assurance instruction: rapid network construction and evaluation, in-class explanation by instructors, out-of-class exploration by students, the ability to develop scenarios emphasizing particular topics, and the ability to reach a large audience.

References

MIL3. OPNET Modeler. OPNET Technologies. Available online at <http://www.mil3.com/products/modeler/home.html>. Last accessed May 5, 2003.

Uiterwijk, A. (1999). Security Game: Playing for Keeps. Federal Computer Week. December 20, 1999.

VanPutte, M. SimSecurity - Distance Learning and Virtual Laboratory for Information Assurance. The MOVES Institute, Naval Postgraduate School. Available online at <http://www.movesinstitute.org/OpenHouse2001/Presentations/VanPutteSimSecurity.ppt>. Last accessed May 5, 2003.

Ressler, S. West Point Bridge Design Contest. Department of Civil and Mechanical Engineering, USMA. Available online at <http://bridgecontest.usma.edu/>. Last accessed May 5, 2003.

Lathrop, S., J. M. D. Hill, et al. (2003). Modeling Network Attacks. Behavior Representation in Modeling and Simulation (BRIMS 2003), Scottsdale, Arizona.

Sun Microsystems. Java WebStart. Available online at <http://java.sun.com/products/javawebstart/faq.html>. Last accessed February, 2002.