Proceedings of the 2001 IEEE
Workshop on Information Assurance and Security
United States Military Academy, West Point, NY, 5-6 June, 2001

A Framework for an Information Warfare Simulation

Donald Welch, Greg Conti
United States Military Academy
{don-welch | gregory-conti }@usma.edu

Jack Marin
BBN Technologies
jmarin@bbn.com

Abstract

In this paper we propose, justify, and outline a framework for an Information Warfare Simulation. We believe such a simulation would allow information security specialists to better test and evaluate concepts and tactics prior to the costly process of developing information security systems. We present a framework for an event-driven, stochastic, high level Information Warfare Simulation. Our framework uses partially ordered discrete events as the building blocks of the simulation. The simulation model is object based, and the four primary categories of objects are Node Address, Connection, Interaction, and Infotron. We introduce the term and concept of an infotron as a means to measure the "goodness" or relevance of information on a network without having to resort to information theory concepts. We describe the construction of a crude prototype information warfare simulation, and present analysis from two example scenarios.

1. Introduction

Military planners employ simulations in training, testing, research and development. For example, suppose a ballistics engineer wants to evaluate the impact on the battlefield of a tank equipped with a larger main gun firing a larger round (bullet). Rather than fit a tank with a larger main gun and produce the new tank ammunition at the cost of millions of dollars, force developers would first test the concept in a force-on-force ground simulation. An event-driven simulation would allow analysts to evaluate the tank against different enemy forces, on different terrain, and in different scenarios. Parameters such as weight, time to load, and time of flight of the larger tank round, along with the ballistics characteristics of the larger round would be entered into the simulation. The effectiveness of the larger tank round would be ascertained with measures of effectiveness such as casualties inflicted on the enemy, the number of enemy and friendly tanks incapacitated, and the speed at which victory (or defeat) is obtained. Based-on the performance of the tank with the larger main gun in simulations, decision makers are better equipped to determine if the new tank design is effective.

We believe it is possible to construct an Information Warfare simulation to provide information assurance professionals with the same type of information that combat simulations provide traditional military planners. This type of simulation would provide information concerning the viability of network tactics (both offensive and defensive), a means to test new "equipment," and even a means to train network security personnel.

In this research, we present a framework for an event-driven, stochastic, high level Information Warfare Simulation. Note, our framework is not a continuous time, low level (i.e. packet level) simulation to be used to evaluate networks, devices, protocols, loads, and other applications. Rather, our framework involves the interactions of events that occur on a network. For example, our framework does not address the simulation of a packet from one source to another; however, the "event" that a packet containing a password is transferred could be a key event in out framework.

2. Background and Previous Work

Simulation has been applied to military modeling probably since the inception of simulation. The reason for this marriage between simulation and military is quite simply it is more cost effective to test equipment and tactics in a simulation rather than in an actual war. Simulation is an abstraction, where one can combine soldiers, tanks, terrain and firepower to study their interrelationships and composite effects [1]. Information Warfare, in some form, has always been part of warfare. However, we have

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE

uncovered few references that apply the theory of simulation to the domain of Information Warfare.

Most references concerning Information Warfare and simulation use simulation as a methodology to test a concept or theory. For example, Smith and Bhattac Harya [2] use a simulation to assess the performance of firewall placement in a large network. Simulation has also been used to assess network topology and performance [3, 4]. However, the idea closest resembling our Information Warfare simulation is reported in Mostow, et al. [5] who describe an Internet Attack Simulator (IAS) that simulates information attacks directed against networks. The IAS simulates three attack scenarios: Denial of Service, Unauthorized Access, and Spoofing. Underlying the IAS environment is a high-fidelity real-time model of Certain Army communication systems.

3. Justification for an Information Warfare Simulation

In this section, we address the question: Why is an Information Warfare simulation model necessary? In section 4, we develop our framework for an Information Warfare simulation, and in section 5 we discuss our initial prototype construction as a proof of principle. That is, we demonstrate our proposed framework is appropriate for building an information warfare simulation.
A network is a complicated system where interactions occur on many levels, many of which are stochastic in nature. With this thought in mind, we next develop several ideas addressing where an Information Warfare Model might be applicable. Throughout this section on model applicability, we will draw comparisons to land combat simulations to illustrate how simulations have been used in the military modeling domain.

Land combat simulations have been used to assess tactics and equipment, identify choke points, evaluate enemy attack plans as well as evaluate defense in depth. Consider an attack plan as an example. Currently, many organizations employ "red teams" or tiger teams to attempt to penetrate the security of systems in order to ascertain the strengths and weaknesses of the system security [6, 7, 8]. For example, the U.S. Department of Defense has used red teams to assess its computer security in an exercise called "Eligible Receiver" [9, 10], while Jonsson and Olovsson [11] used undergraduate students as red team members to build quantitative models of the intrusion process. We can compare red teams to the red force that Army units train against at the National Training Center. While the experience gained from training against live forces is unmatchable, the data generated from these real training exercise is miniscule when compared to the data generated form force-on-force simulations. However, red teams are manpower intensive and generate little useable data when compared to properly constructed simulations.

An Information Warfare simulation could assist in evaluating proposed system specifications, even those that are considered impossible to implement using today's technology. Earlier we described how force developers might use a ground force simulation to assess the impact of a larger tank munition. Similarly, given a limited budget, would a better investment for technology developers to createfirewalls that are 95% accurate with a 2% degradation in network performance, , 100% accurate intrusion detection with a specified time lag, unbreakable encryption, or single network sign-on? A properly crafted simulation would estimate the pay-off of these goals before committing to formal development.

4. Simulation Framework

Our simulation framework uses partially ordered discrete events to run the simulation. Driving reasons why we selected this methodconcern the efficiency of partially ordered discrete events. A continuous simulation would be very costly to implement. The nature of Information Warfare is such that there are brief periods of intense activity interspersed by long periods of almost no activity. The time fidelity is 1 millisecond. Events are placed on the event queue to the nearest millisecond. Events that have the same simulation time may be processed in any order. Some of the events that occur on a computer network must occur sequentially while others have absolutely no effect on each other. Hence, for efficiency we use partially ordered discrete events. Additionally, partially ordered discrete events can interact with simulations of the physical world as stipulated by the Department of Defense standard High-level Architecture (HLA).

This simulation model is object based. We model entities in the simulation using the object model. Each entity has attributes and behaviors. The are four major categories of objects:

1. Node Address
2. Connection
3. Interaction
4. Infotron.

With these four types of objects, we can model Information Warfare at the entity level.

4.1. Node Address

When simulating the physical world, there are many different types of platforms: aircraft, ships, trucks, etc.

Even though they have widely different functions they interact with the world in the same way. They move and interact constrained by the terrain and other platforms in the simulation. Node Addresses are the corollary in cyberspace. A Node Address object is used to identify and simulate nodes on a network that receive, process or transmit information such as workstations, servers, and routers. A Node Address object simulates any component of the network that has an address of some sort.

The attributes of a Node Address include the basics such as processor, memory, drive space, and operating system. They also include the configuration, which includes the services running. The behaviors are coded into a Node Address. Some behaviors start actions. For example, at time 20 a client initiates a Telnet session with a server. Some behaviors are reactive. An example would be a firewall that receives a HTTP request from a client on the outside for a server on the inside. Based on its configuration (attributes) it would then pass on the HTTP request or refuse it.

4.2. Connection

A connection object simulates physical links between node objects. In a force on force simulation, connection objects would be the. For example, two tanks cannot see or shoot at each other if there is a hill in between them. Connection objects include channels and network components, such as hubs that do not have an address. Connection objects limit the ways that Node Addresses interact in the simulation. A client and server cannot exchange information without some series of connection objects that form a path between the two. The key parts of connection objects are their attributes. The attributes define the connection, its speed, reliability, etc. The behaviors of connection objects are very simple.

4.3. Interaction

Interaction objects simulate the exchanges of information between nodes on the network. Again, drawing on the battlefield simulation analogy, we are not trying to simulate every communication between platforms on a battlefield. Rather, we concentrate on a higher level, notable events that may have some future impact on the network. This exchange is at a macro level, and does not necessarily involve packet level information. A HTTP transaction for a series of web pages is an example on an Interaction.

Interactions are a way of abstracting actions with numerous parts into objects we can more easily reason about. The key to implementing interactions is understanding the purpose of the interaction or the behavior.. Also, interactions are useful to group a sequence of actions in an intelligent way. Interactions can simulate a fairly small occurrence in a network like a user access, or a very large event like a port scan against a sub-net. or abstract all the network traffic involved in a remote buffer overflow attack into a single object. .

4.4. Infotrons

Infotrons represent the smallest pieces of information that are of interest to the simulation. A database could be simulated by a single Infotron object or by many Infotron objects depending on the purpose of the simulation. Infotrons have no corollary in the physical world. Users determine success by looking at the number of enemy and friendly destroyed and the disposition of the forces. Did we take the hill? In information war the objective is information. Did the good guys maintain all five security services for their key information? Did they breach the integrity of the bad guys key information? These are the types of questions that we need to answer in cyberspace. To do so we have to explicitly identify and simulate key information. The simulation framework does not try to simulate the value of information, but rather to include user determined values in the simulation.

Infotrons are the key determinants of success. Applying the CIA+ taxonomy for information (confidentiality, integrity and availability, non-repudiation and authentication), the simulation we propose will tell users the the attacker did or did not breech the confidentiality, etc. of the Infotron object. Because simulations are useful in predicting complex interactions, an attack on one Infotron object may cascade to other Infotrons throughout the simulation.

5. Example Simulation Models

5.1. Example 1: Sniffing A Password

Below is a trivial example of an information operation. We will use this example to step through the simulation of the attack to better explain the framework and provide some insight of the usefulness of a simulation of this fidelity when expanded to a non-trivial level. The trivial

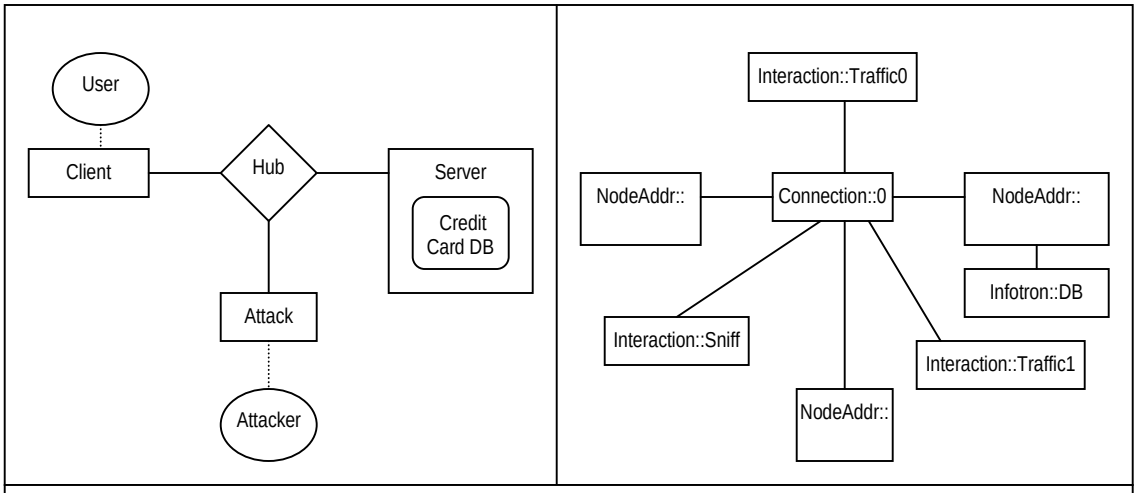

Figure 1: The diagram on the left represents the scenario. The right side shows the objects used to simulate the scenario and the paths between the objects. Each object is designated with its class name or type first separated from the instance name by the double colon. This is the configuration at the start of the execution. The paths may change, for example as a copy of the DB moves to the Client there will be a path between the DB Infotron and the Client.

example is a client and server that are connected through a network and an attacking workstation that is running network sniffer software on that network link. The critical information is a list of customer credit card numbers that reside in a database on the server.

The infrastructure is modeled with three Node Address objects: client, server and attacker. There is one connection object that simulates the hub and three cat 5 cables that link all three systems together. The database is modeled by a single Infotron because access to any part of it is equally bad for the database owner. There are two Interactions modeled in this example. The first, is the traffic that passes back and forth between the client and the server. Sometimes it carries unencrypted passwords for the server; sometimes it carries credit card information or the Credit Card Infotron as the client accesses the database. The second, is the sniffing of the network.

The simulation starts at T_0. This instantiates the four infrastructure objects and these objects start to exhibit their *run* behaviors. The Client as part of its *run* behavior creates and starts a new interaction object named Traffic. This object uses an algorithm to simulate the traffic and more importantly the authentications that pass between the Client and Server. To do this it will place events on the queue in the proper distribution of the proper type. For example, at T_{15} an unencrypted telnet login crosses the connection object.

The Attacker node is simulating an attacker that wants to sniff some passwords but not get caught. Therefore, the sniffer is only running during specified time periods. During these periods, the sniffer checks the event queue for items of interest. Passwords and Infotrons are items of interest to this attacker. During the first period that the sniffer is operating, no information of interest is passed on the connection. However, the second time that the sniffer is active, the Traffic interaction places an unencrypted password event on the queue. The sniffer interaction picks this event up and passes it to the Attacker. The Attacker's behavior differs based on the results of each sniffer interaction. In the first case, the attacker simply scheduled another sniffing period. In this case, the Attacker did not have to decrypt the password, so it instantiated a Traffic interaction. This traffic interaction used the sniffed password to get authorized access to the Credit Card Infotron.

Once the simulation is complete, the simulation user can determine the security of the Infotron. Did it maintain its confidentiality, integrity, availability, non-repudiation, and authentication throughout the simulation execution? If not, at what time were any of these breached and how were they affected. Since each simulation execution is non-deterministic, through multiple executions, a picture of the system security will emerge. Not only will it portray the

likelihood that security of the Infotrons will be maintained, but the ways that each Infotron might be open to attack.

5.2. Example 2: Defense in Depth

Our second example is more complex and tests the effectiveness of a firewall-based defense in depth. It simulates an attacker, five targets and a firewall. In addition to the primary firewall, each target system is equipped with a host-based personal firewall. The attacker's goal is to penetrate the primary firewall and capture the information located on each of the target systems. We wish to use the model to perform a risk assessment and cost benefit analysis of the network's security using a variety of product configurations. The attacker will try to execute ftp on each target system through the primary firewall. If successful, the attacker will then attempt to penetrate the host-based firewall on each of the target systems. Each personal firewall could be configured differently, so our attacker will need to attack each target system with an independent probability of success. If successful at penetrating the host-based firewall on a given system, the information is considered compromised.

We do not know the exact characteristics of each firewall product under all circumstances, but we believe that it is reasonable to expect that we would know something about each product. This knowledge is shown as a general percent effectiveness against an ftp attack as well as a product cost. We will execute the simulation multiple times (n=10,000) against each of the 16 possible combinations of the products listed in Figure 2.

Primary Firewall		**Personal Firewall**	
Effectiveness	Cost	Effectiveness	Cost
50%	$200	50%	$30
75%	$500	75%	$50
90%	$1000	90%	$100
99%	$2,500	99%	$200

Figure 2: Firewall Effectiveness

To simulate the infrastructure we use a group of seven node address objects: the attacker, firewall and five targets. There are two connection objects this time: one between the attacker and firewall and one between the firewall and the group of targets. Note that the second connection object includes the hub because it does not have a network address. The connection object also contains pointers from the firewall node address object to the node address object representing each target. This utilization also demonstrates the flexibility of the connection object to act as a convenient mechanism for abstracting away unneeded detail by grouping related network communications infrastructure. Each target workstation uses an infotron object to represent the information that the attacker wishes to capture. We do not assign an arbitrary value to each infotron, but the capture of infotrons does represent a decline in the CIA of the network. The diagram of this scenario is depicted below in Figure 3.

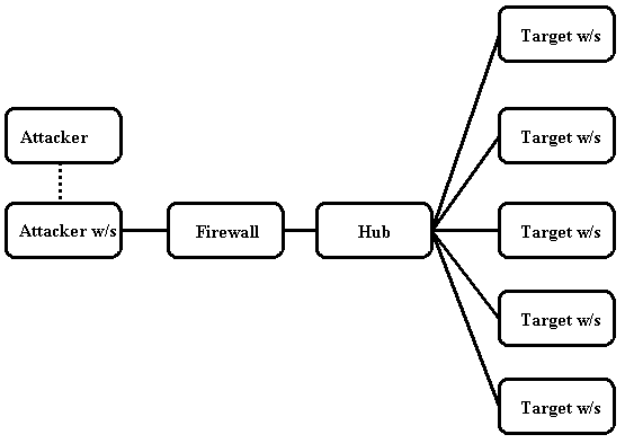

Figure 3: Diagram of the Firewall Scenario

After the simulation starts, the attacker creates an interaction object to simulate the ftp session. The attacker knows the address of each target but does not have to know that a firewall is in between. The connection object contains the information that the targets are connected to it. There are two potential outcomes in this scenario.

The primary firewall is successful at defeating the attack. The attacker begins an ftp based attack against the primary firewall. An interaction object is created associated with the connection object between the attacker's workstation and the firewall. In this situation, the firewall is successful at defeating the attack, it stops the ftp interaction and the simulation is over.

The primary firewall is breached, and 0-N host-based firewalls are breached. The attacker begins an ftp based attack against the primary firewall. An interaction object is created associated with the connection object between the attacker's workstation and the firewall. The firewall is successfully breached by the attack and the interaction object now expands to include association with the connection object between the firewall and each target workstation. The attacker then attempt to bypass the host-based firewall on each target. If successful on a given system, the target returns the infotron through the simulated ftp session to the firewall. The firewall passes

that information to the attacker through the original ftp interaction. The attacker then moves on to the next target. If the attack on a target was unsuccessful, the attacker then moves on to the next target. In both cases, when all targets have been attacked. The attacker then terminates the ftp interaction and the simulation is over.

5.3. Results (Insights gained from the simulation)

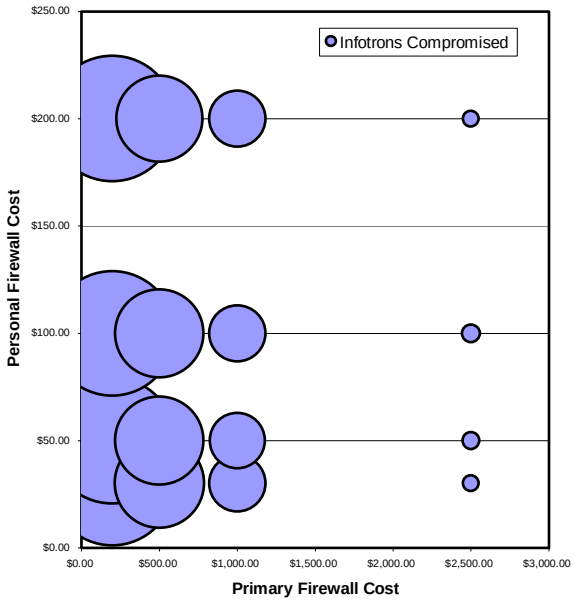

Figure 4: Graph of the Firewall Scenario Results

Figure 4 graphically illustrates the results of the Firewall Scenario. Each bubble is plotted at the X,Y coordinate corresponding to the Primary (X) and Host-Based (Y) firewall cost. The area of each bubble is proportional to the number of infotrons compromised with that network configuration. Therefore, the large bubbles show the greatest number of infotrons compromised. It is clear from the graph which products, used in combination, provided the most successful defense in depth. Analysis indicates the most successful and cost efficient defense is to use a higher quality firewall at the network access point. The quality of the host-based firewall is of lesser importance. The simulation was also successful at determining the changes in the CIA of the network and each target system, based on the number of infotrons compromised.

The following is a summary of other results:

- Increased fidelity can be gained in many aspects. For example, some algorithm could be developed to simulate the false alarm rate of each product.
- The simulation provided potentially counterintuitive results. It was not clear from observation what the best combination of products would be.
- The model has the ability to scale. For example, it would be trivial to change the number of target workstations from 5 to 500 and rerun the simulation.
- The model will support variants. Changing characteristic of the objects modeled would allow for significant flexibility.
- We were able to estimate the amount of resources expended.
- The model can help validate small parts and them compose the results and help form a more understood, larger whole.
- Some results from trivial scenarios can appear to be obvious, but when the user scales the model upward and sets up a number of variant simulations the results can far outpace what a human can do manually.
- The simulation was successful at determining the best combination of primary and host-based firewall products that were most successful at protecting the information in the most cost efficient manner.
- Simulation can increase understanding of the problem domain, but the output is not a clean number. Human intelligence is still required to analyze the data and spot trends.

This example helps to illustrate the approach we have taken. The framework must scale in that it must be able to simulate attack components to more easily synthesize new attacks. It must also simulate attacks in whole, so that large infrastructures and battles can be modeled. The simulation must be useful in simulating information warfare completely in cyberspace as well as simulating the effect of information warfare on the physical world.

6. Conclusion and Future Work

Taking a snapshot of future developments in the field of Information Security, we see topics such as the expansion beyond firewalls and PC's to IP enabled toasters, Quantum Computers, tamperproof hardware, Internet II

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE

(infrastructure built with security in mind), traffic analysis and network camouflage, and fingerprinting nodes. However, what is missing is a method to examine and compare the possible effectiveness of these future techniques.

In this paper, we describe; present and justify the idea of a high-level Information Warfare simulation. We describe a framework that uses partially ordered discrete events as the building blocks and we describe the objects associated with this framework. We also introduce the term infotron as a means to assess the value of information on the system. Finally, we describe the construction and applicability of a proof of principle prototype.
Future work will involve extending the initial prototype to simulate an actual network, such as the Information Warfare, Analysis, and Research (IWAR) laboratory [12] at the US Military Academy.

.

7. References

[1] Hughes, W., "Overview of Military Modeling" in *Military Modeling* (Hughes, W., ed), Military Ops. Research Society, 1988.

[2] Smith, R and Bhattac Harya, "Firewall Placement In a Large Network Topology," in *Proc. 6th IEEE Workshop on Future Trends of Distributed Computing Systems*, 1997.

[3] Breslau, L., et al., "Advances in Network Simulation," *Computer*, Col. 33, No. 5, May 2000.

[4] Optimum Network Performance, OPNET Modeler, http://www.opnet.com/products/modeler/home.html, March 2001.

[5] Mostow, J., Roberts, J., and Bott, J., "Integration of an Attack Simulator in an HLA Environment," *Proc. IEEE Systems, Man, and Cybernetics Workshop*, West Point, NY, June 2000.

[6] Parker, D. *Fighting Computer Crime*, Wiley and Sons, NY, pp. 393-395, 1999.

[7] Herschberg, I. "Make the Tigers Hunt for You," *Computers and Security*, vol. 7, pp. 297-203, 1988.

[8] Goldis, P. "Questions and Answers about Tiger Teams," *ED-PACS, The EDP Audit, Control, and Security Newsletter*, vol. 27, no. 4, pp. 1-10, 1999.

[9] CIWARS Intelligence Report, Center for Infrastructal Warfare Studies, June 21, 1998

[10] Gertz, B. "Computer Hackers Could Disable Military; System Compromised in Secret Exercise," *The Washington Times*, April 16, 1998

[11] Jonsson, E. and T. Olovsson, T. "A Quantitative Model of the Seciurity Intrusion Process Based on Attacker Behavior," *IEEE Trans. on Software Engineering*, vol. 23, no. 4, pp. 235-245, 1997.

[12] United States Military Academy, Department of Electrical Engineering and Computer Science, Information Technology and Operations Center, Information Warfare Laboratory, http://www.itoc.usma.edu/iwar.html, March 2001.

ISBN 0-7803-9814-9/$10.00 © 2001 IEEE