

Simulation to Support Security Issues Related to System Interoperability

John A. “Drew” Hamilton, Jr., Ph. D.
Computer Science and Software Engineering
Room 107 Dunstan Hall
Auburn University, AL 36849-5347
hamilton@eng.auburn.edu
<http://www.drew-hamilton.com/>

Keywords: Security, Interoperability, Network Simulation, Worms, OPNET

Abstract

Interoperability, as defined in the IEEE Standard Glossary of Software Engineering Terminology, “is the ability of two or more systems or components to exchange data and use information.” There are significant technical issues associated with communication system interoperability. In military communications, significant non-technical issues relating to national security policy and release authority also come into play.

Once coalition networks are established, the vulnerability of information systems may increase. Internal propagation of a worm with the characteristics of say “Nimda” or “Code Red” can generate internal broadcast storms behind the network firewalls. There are significant limitations to applying simulation information security issues. Most security vulnerabilities occur at the end points and evaluating the actual systems best assesses these vulnerabilities. However, network simulation is an obvious choice for evaluating the impact of primary and secondary packet storms on large, internal networks.

This paper will outline issues associated with communication system interoperability, the security vulnerabilities associated with improved interoperability, network simulation to support the evaluation of the effects of worm-induced packet storms and the experimental design, implementation and results using the OPNET simulation environment.

INTEROPERABILITY

Communication system interoperability, the ability of two or more systems or components to exchange data and use information [IEEE 1990], is inherently software-based. Interoperability implies the existence of diverse systems that need to exchange data and services. Much is written about “systems of systems.” System interoperability is what makes heterogeneous systems of systems a reality. All of these systems are composed of hardware and software.

Hardware is not easily changed. Furthermore, fielded hardware systems often cannot be wholly replaced.

Diverse hardware-based communications systems require an overall software architecture in order to interoperate. As noted in IEEE Standard 12207.0-1996 *Software Lifecycle Processes*, software architecture describes the top-level structure of the over-arching system and describes the software components. Specifically, developers adhering to the standard are required to develop and document a top-level design for the interfaces external to the software item and between the software components of the software item. This is an essential first step in achieving interoperability between any two systems.

In Defense applications, interoperability is seriously hindered by the sheer number of systems, standards, and system developers /procurers. Figure 1 illustrates some, though no means all, of the commands developing/fielding software-intensive communications systems.



Figure 1. Some organizations involved in command system acquisition: DISA, NSA, three service C2 acquisition commands and ten unified commands.

An exemplar “system of systems” is the Global Command and Control System (GCCS) as shown below in figure 2. A key factor in the success of GCCS is the discipline to which interface standards are maintained by the Defense Information Systems Agency. GCCS is a non-trivial system with at least twenty-three systems exchanging information with the top-level GCCS application. Further complicating this

Likewise, we want to control release of U.S. classified information.

To achieve effective combined interoperability, we must develop much more capable security procedures and sophisticated tools to allow information exchange while protecting our national and allied data.” [Blair 2001]

INTEROPERABILITY & SECURITY RISK

As Admiral Blair noted, in the previous GCCS example, the interoperability issue was a policy issue, not a technical issue. Policy and technology together can potent challenges. Consider a requirement US Pacific Command articulated needing a secure email system to exchange sensitive but unclassified information between Headquarters, Australian Theater and Headquarters, US Pacific Command as illustrated in figure 4.



Figure 4. Secure email in the Pacific

The alternatives to secure emails were frequent, incredibly long facsimile messages exchanged over secure telephone lines.

Unfortunately, even limiting data exchange to email applications increases risk to all stations enabled for interoperability. Viruses can spread through email so the more stations connected, the greater the risk for attack. Worms, malicious programs specifically designed to replicate across networks are continuing threat.

The Morris Worm, which attacked networked stations in October 1988, was extensively documented [Spafford 1989] and [Rochlis & Eichin 1989]. Although a well-documented phenomena, network vulnerability to worm attacks has only increased. New worms continue to proliferate and virus scanners are updated *after* the initial attacks. Antivirus responses while eventually effective are purely defensive measures.

Stage 1	Local executable file infection (prepending)
Stage 2	Search for IP addresses from registry
Stage 3	Elevate privilege and execute on vulnerable remote computers
Stage 4	Compromise local security settings

Table 1. Lifecycle of a typical Nimda Worm variant.

Thirteen years later, the Nimda Worm demonstrated the vulnerability of modern email systems and webservers. The Nimda Worm was identified on 11 October 2001 and was found to have a four-stage lifecycle as shown in table 1.

Consequently, it is straightforward to plan and execute a timed distributed denial of service attack (DDoS). A distributed denial of service attack is Significant effects have been achieved through ad hoc, and sometimes amateurish attacks.

[King, Dalton & Osmanoglu 2001] note that there are many variants of denial of service attacks such as:

- Programming mistakes that take 100% of CPU time.
- System memory usage may continually increase due to a memory leak.
- Malformed data requests such as Web requests or remote procedure calls (RPCs).
- Large packets such as email addresses and Internet Control Message Protocol (ICMP) requests.
- Non-stop network traffic User Datagram Protocol (UDP) and ICMP (broadcast storms and network flooding).
- Forging routing information or unresponsive connection requests.
- Incorrectly configured wiring, power, router, platform, or application.

The authors further note that the Computer Emergency Response Team (CERT) has documented more than 318 DoS attacks.

A distributed DoS is merely the employment of a distributed set of remote computers to intensify the impact of the attack.

An DDoS attack launched in conjunction with an email-propagated worm with a specific military objective could successfully “jam” military computer networks at a critical time at the attacker’s choosing.

Consider the following attack scenario:

1. Select desired date/time for denial of service attack initiation in worm payload.
2. Study resources on the internet to assist in the design of the worm.
3. Use lessons learned from various white hat and black hat security sites to maximize surprise elements of worm.
4. Use “human engineering” to ensure that worm is introduced undetected on as many target machines as possible.

5. Reinforce DoS attacks remotely through any backdoors opened by the worm at h-hour.

Even if the target network is only affected for a few hours, it may be a militarily significant impact. It is a reasonable precaution to evaluate network vulnerabilities to DoS/DDoS from internal as well as external stations.

NETWORK SIMULATION AND DDoS VULNERABILITIES

Four graduate students at Auburn University undertook a serious look at one network on campus. After modeling the network in OPNET, one pair of students studied the predicted impact of increased multimedia traffic on the network while the other pair focused on evaluating the impact of DoS attacks on the network.

OPNET may be described as a communications-oriented simulation language. The name OPNET is derived from Optimized Network Engineering Tools. The single most significant aspect of OPNET is that it provides direct access to the source code coupled with an easy-to-use front end. This capability allows the introduction of multiple traffic sources, from PDFs, from network emulators and from observed traffic.

OPNET uses the following modeling hierarchy as shown in figure 5 [Hamilton, Nash & Pooch 1997]. The students used node models to represent the CISCO 5500 switches found in Auburn’s Broun Hall as shown in figure 6.

Network Models	networks and subnetworks
Node Models	individual nodes and stations
Process Models	STD that defines a node

Figure 5. OPNET model hierarchy.

Broun Hall has four layer three switches that handle all of the traffic between the internal computers. Three of these connect to a main switch via gigabit fiber optic cable. The main switch connects to the main campus switches via gigabit fiber optics as well.

The students modeled the switches as follows: Each wiring closet was represented by a single switch, each LAN by a single node, and RoTW represented

the source/destination of all inbound/outbound traffic respectively.

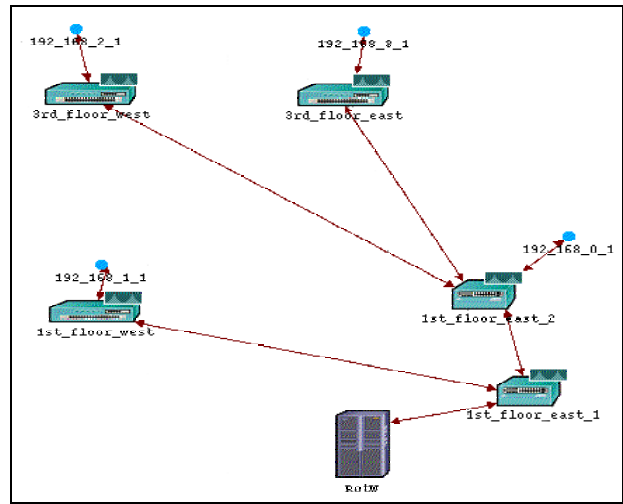


Figure 6. Topology of the Broun Hall network as simulated using OPNET [Rouse & Tidwell 2002].

The students used Sargent’s work [Sargent 1998] as a guide to validate their model. Validating and verifying their model was the hardest part of their project.

Verification of a simulation is the process of assessing the degree to which the implementation transforms inputs into outputs *as specified by the model*. The ultimate verification test is to model a known system and run the same sets of inputs through the actual system and the simulation. If the results are statistically the same, then you have reasonable assurance that you have implemented the model correctly.

This was the approach used by the students. Using data collected by the College of Engineering. In the course of the experiment, the students learned first-hand that network monitoring is a non-trivial effort. In trying to verify the model, it was subsequently determined that the actual time scale of the network monitoring system was not properly understood by the system administrator. The students successfully verified that their model accurately represented the actual network for a given load.

Validation is the process that establishes the extent to which a model does (or does not) acceptably represent the phenomenon of interest. Once we know we have a good model, how do we gauge its predictive power? Generally a good traffic model is necessary for a network simulation to achieve any meaningful predictive power. Network traffic patterns cannot be relied upon to follow a standard probability

distribution. The failure of Poisson processes to model network traffic is outlined in [Paxson & Floyd 1995].

Accurate modeling of network traffic can limit many network simulation studies, but is not an issue in modeling DoS attacks. For a given worm, it is possible to exactly replicate the initiation time and traffic volume of each infected node. Network simulation is particularly appropriate for studying large-scale distributed DoS attacks since it is usually too costly to use large distributed systems for live DoSD/DoS testing.

Both student groups wanted to see the effects of increased traffic on the network topology. They used the built-in traffic scaling functionality of OPNET to scale our traffic with 1000% and 5000% increases [D'Amico & Taylor 2002]. Increasing traffic beyond 5000% overwhelmed the network.

The network the students selected to study was very lightly loaded, usually averaging traffic of 3.5 megabits/sec percent loaded based on the data collected by the university network staff.

The students observed that the Cisco switches had greater capacity than the gigabit links. The Cisco white paper regarding the Cisco 5500 switch, rates the switch at 50 Gbps maximum throughput. The technical specifications of those switches were found below at:

<http://www.cisco.com/univercd/cc/td/doc/pcat/ca5000.htm>.

It was clear that there were simply not enough gigabit links feeding into the switches to overload the switches, thus the throughput on the links was the theoretical throughput limit.

The teams reported the following results: Figure 7 shows that the throughput (bits/sec) maxes out at 1 Gbps.

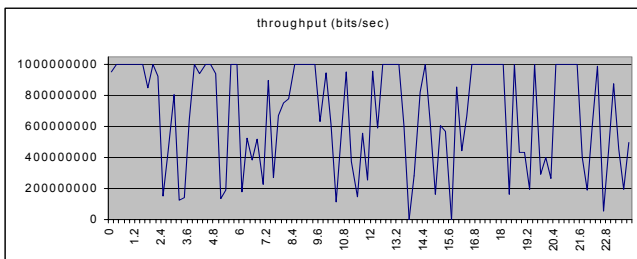


Figure 7. Throughput limited to 1 Gbps.

This is expected because the gigabit link can have no higher capacity than its rated capacity of 1 Gbps. Consequently, in figure 8 the students observed that utilization behaves in direct proportion to maximum capacity.

Based on this study several conclusions were drawn regarding the vulnerability of the network to an internal DoS/DDoS attack. First it was observed that

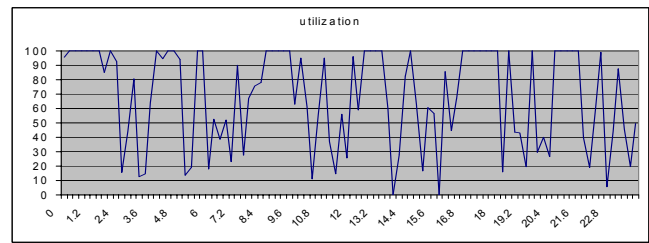


Figure 8. utilization behaves in direct proportion to max capacity.

the network was generally very lightly loaded. Second it was observed that each switch had significantly greater processing capacity than a single gigabit connection. Given the current topology (to include the limited number of stations on the network), it would be very unlikely to that an internal DoS attack could overwhelm a switch. However individual link failures could be expected.

CONCLUSION

Those pundits who glibly extol the virtues of commercial-of-the-shelf (COTS) hardware and software to the Department of Defense should seriously reconsider their arguments. The same COTS hardware and software enables potential adversaries to rehearse attacks against DOD systems in the same manner that we used to assess our own vulnerability.

Modeling and simulation is clearly becoming a mainstream tool in many domains. However, the nature of computer/network security issues is such that often it is best to simply work with the actual systems rather than trying model those systems. Effectively modeling buffer overflow attacks requires a high fidelity model. Testing and evaluating the actual systems seems a better strategy.

However, network simulation is a mature, mainstream tool for the study and evaluation of networks. It is simply too costly to flood operational networks and measure the results. A validated network simulation is clearly a more practical means of evaluation.

System interoperability is a force multiplier for command and control systems. But added capability increases risk. More connected stations increases the risk. Assessing the vulnerability of a network to DDoS attacks is prudent. Ken Rouse and Chris Tidwell at Auburn University have demonstrated one practical means to evaluate such vulnerabilities using OPNET.

REFERENCES

[Blair 2001] Blair, Admiral Dennis C., Commander-in-Chief, US Pacific Command, Statement before the

US Senate Armed Services Committee, 27 March 2001.

[D'Amico & Taylor 2002] D'Amico, Jean, Taylor, Brandon, Term Paper, "Simulating Broun Hall: An OPNET Experiment," COMP 8700, Simulation of Computer Networks, Auburn University, Spring 2002.

[Hamilton, Nash & Pooch 1997] Hamilton, J.A., Jr., Nash, D.A., Pooch, U.W., *Distributed Simulation*, CRC Press, Boca Raton, Fla., 1997, pp 332 – 338

[IEEE 1990] IEEE Standard 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*, Institute of Electrical and Electronics Engineers, Piscataway, NJ, p 42.

[King, Dalton & Osmanoglu 2001] King, Christopher M., Dalton, Curtis E., Osmanoglu, T. Ertrem, *Security Architecture*, RSA Press, Osborne/McGraw-Hill, New York, 2001, p 455.

[Meinel 2001] Meinel, Carolyn, "Code Red for the Web," *Scientific American*, October 2001, pp 42 – 51.

[Paxson & Floyd 1995] Paxson, V. and Floyd S., "Wide Area Traffic: The Failure of Poisson Modeling," *IEEE/ACM Transactions on Networking*, no. 3 (June) 1995, pp 226 - 244.

[Rochlis & Eichin 1989] Rochlis, Jon A., Eichin, Mark W., "With Microscope and Tweezers: The Worm from MIT's Perspective," *Communications of the ACM*, Association of Computer Machinery, New York, vol. 32, no. 6, pp 689 – 698.

[Rouse & Tidwell 2002] Rouse, Ken, Tidwell, Chris, Term Paper, "Simulation of a DoS Attack on a Real System," COMP 8700, Simulation of Computer Networks, Auburn University, Spring 2002.

[Sargent 1998] Sargent, Robert G., "Verification and Validation of Simulation Models," Winter Simulation Conference, Washington DC, December 13-16, 1998.

[Spafford 1989] Spafford, Eugene H., "Crisis and Aftermath," *Communications of the ACM*, Association of Computer Machinery, New York, vol. 32, no. 6, pp 678 – 687.

[Summers 2001] Summers, Major Paul, Director, Joint Forces Program Office, Space and Naval Warfare Systems Command, San Diego, Calif. Unpublished correspondence with the author.

Author

John A. "Drew" Hamilton, Jr., Ph.D., is an associate professor of computer science and software engineering at Auburn University. He has a B.A. in Journalism from Texas Tech University, an M.S. in Systems Management from the University of Southern California, an M.S. in Computer Science from Vanderbilt University and a Ph.D. in Computer Science from Texas A&M University. Prior to his retirement from the US Army, he served as the first Director of the Joint Forces Program Office and on the Staff and Faculty of the United States Military Academy. CRC Press publishes his book, *Distributed Simulation*, written with Lieutenant Colonel David A. Nash and Dr. U. W. Pooch. Web page: <http://www.drew-hamilton.com>