

Network Vulnerability Analysis Tool Precis

Stephen F. Bush

Stephen F. Bush, General Electric Corporate Research and Development, KWC-512, One Research Circle, Niskayuna, NY 12309 e-mail:
bushsf@crd.ge.com

March 29, 1999

DRAFT

Abstract

This precis describes a tool for quantifying the vulnerability of a communications network. It is important that information warfare studies include both offensive and defensive strategies in an integrated manner since neither can be studied in isolation. It is assumed that an attacker has a finite amount of resources with which to discover faults in the network security of a data communications network and that each fault discovery consumes the attackers' resources. Network security actions may be taken to increase security in strategic areas of the network and to actively deter an attack. Reactions such as these by network security in response to an attack have a both a monetary cost and a cost in terms of reduction of network resources and degradation of services to network consumers. An optimal course of action by network security in response to an attack is to minimize network access to an attacker while also minimizing the impact to legitimate network consumers. This requires precise assessment of network security vulnerability and quantification of effects on network consumers by actions taken by network security in response to an attack. This white paper proposes incorporating methods and algorithms into an existing proto-type tool that we have developed for using vulnerability information collected from an actual network and simulating the results of an attack so the command and control strategies can be studied.

Keywords

Information Warfare Strategy and Control, Network Security, Vulnerability Analysis.

I. OVERVIEW

Communication network security vulnerabilities have been studied at GE CR&D using a Network Insecurity Path Assessment Tool (NIPAT) [1] that has served as experimental validation of a variety of techniques to analyze a communications network for vulnerabilities. In this precis, we describe the capabilities of the network vulnerability system without revealing its enabling intellectual property.

As an example of Network Insecurity Path Assessment Tool's current capabilities, Figure 1 displays 2,000 vulnerabilities found on a few nodes of a network that were thought to be reasonably secure. Vulnerabilities are displayed by host and type. The number along each edge of the graph represents the number of opportunities available to the attacker to reach the next vulnerability. Using this information, Network Insecurity Path Assessment Tool has several algorithms for determining the vulnerability, V .

The Network Insecurity Path Assessment Tool uses two fundamental techniques for determining vulnerability to attack. Both techniques are based on determining "insecurity flow". The Network Insecurity Path Assessment Tool can display the results at various levels of detail including the individual host level, vulnerability types, host types, or individual vulnerabilities.

Clearly, Network Insecurity Path Assessment Tool provides valuable vulnerability information for any communications network. However, it can be taken a step further by adding the capability of automatically determining the placement of security safe-guards, S , given cost limitations, L . Finally, Network Insecurity Path Assessment Tool can be enhanced with the ability to determine optimal automatic rapid-response control measures to counter an attack, given the constraint of minimal impact upon users. Enhancing Network Insecurity Path Assessment Tool with the optimal placement of security safeguards and response to attack are the subject of this white paper.

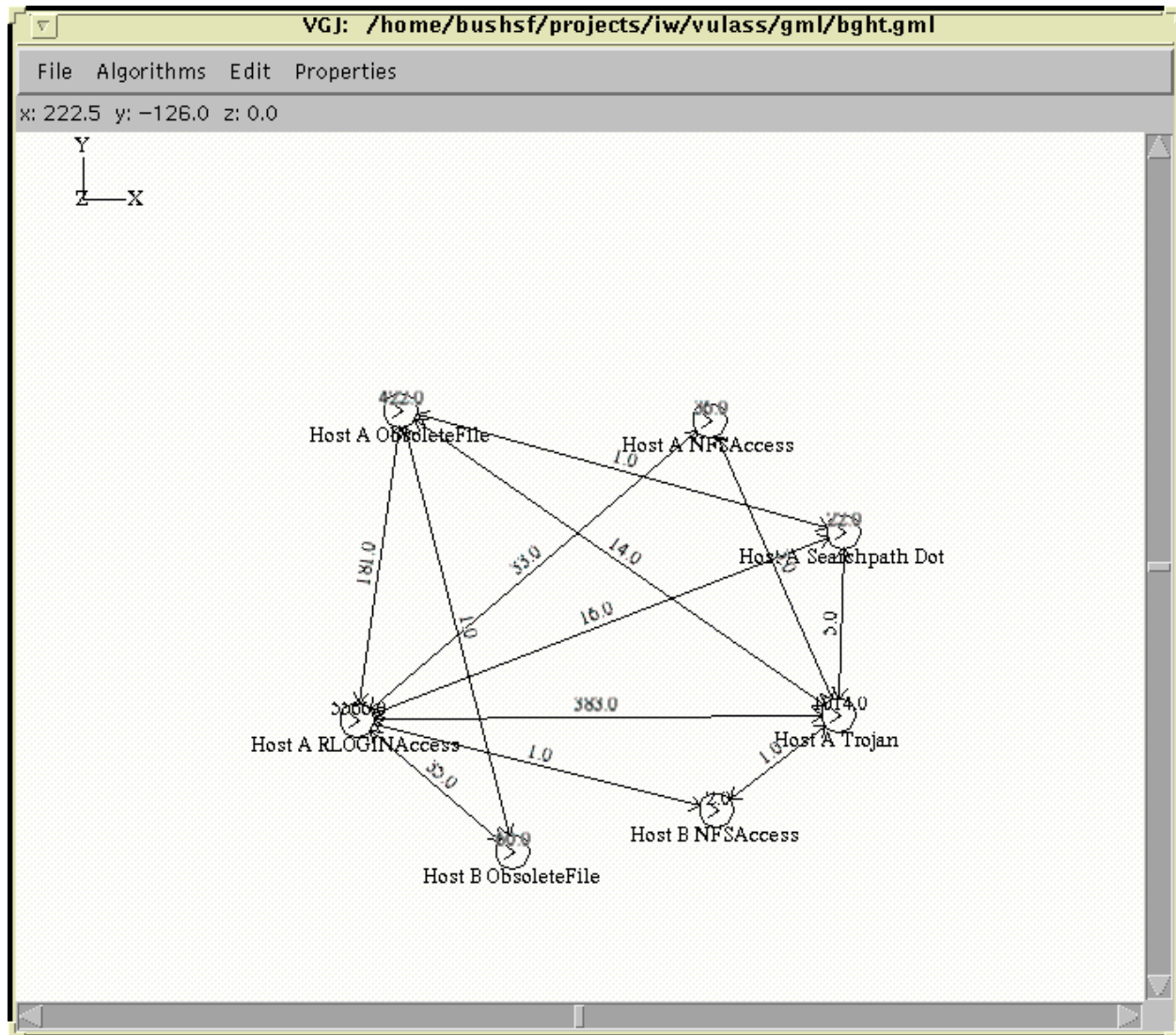


Fig. 1. An Example Vulnerability Graph.

II. AUTOMATIC SECURITY SAFEGUARD PLACEMENT AND CONTROL

It becomes clear that defensive security safeguards cannot be studied independently of offensive information warfare. Thus, a tool which can accurately study both is required. Initially, perfect information is assumed to be available to both the attacker and defender. Later in this paper, we consider the effects of the more realistic case of imperfect information, since neither the attacker nor the defender can have complete knowledge of one another's state.

Using the Network Insecurity Path Assessment Tool tool and analysis methods, a network security analyst can allocate security safe-guards in order to minimize the entire network vulnerability, or to minimize the vulnerability from known attack points to particular targets.

First, from a fundamental network vulnerability flow viewpoint, the strategy of allocating safe-guards in combi-

nations of serial and parallel strategies can be examined. Figure 2 shows the Network Insecurity Path Assessment Tool analyzing an attack from host A to host B. In this case, the number of opportunities have been normalized into probabilities. Figure 3 shows the results as security safe-guards are removed. The solid line is the vulnerability of a single connection from the attacker to the defender having the same vulnerability flow as the links shown in Figure 2. Below a probability of 0.6 the diversity of vulnerability types helps to increase security, but interestingly, above 0.6 it does not.

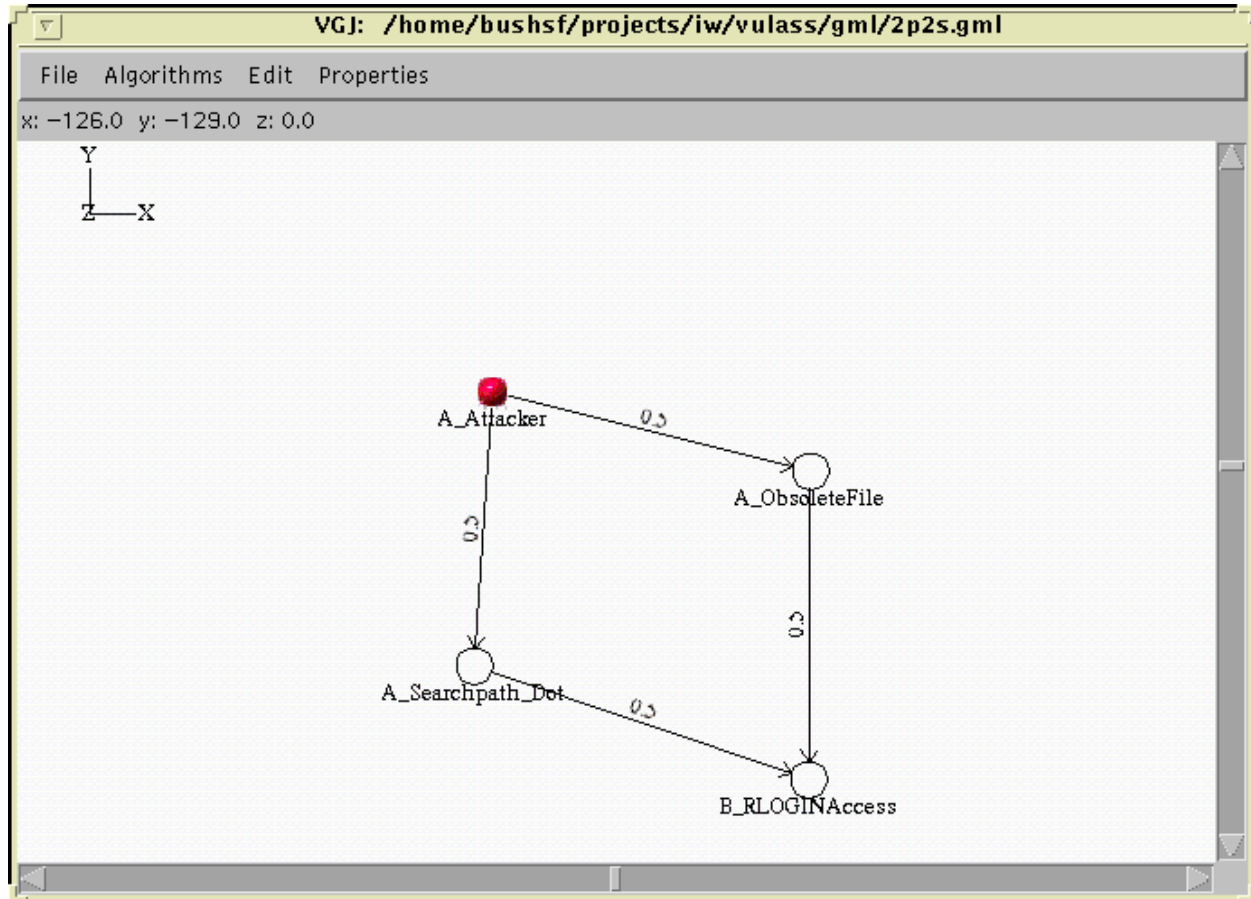


Fig. 2. An Example of Security Safe-Guard Allocation.

III. STRATEGIC CONTROL AND RESPONSE

Once an attack has been detected, the network command and control center can respond to the attack by repositioning security safe-guards and by modifying services used by the attacker. However, cutting-off services to the attacker also impacts legitimate network users and a careful balance must be maintained between minimizing the threat from the attack and maximizing service to customers. For example, various stages of an attack are shown in the Network Insecurity Path Assessment Tool in Figure 4. Since the allocation of security resources never changes throughout the attack, the vulnerability of the target increases significantly with each step of the attack.

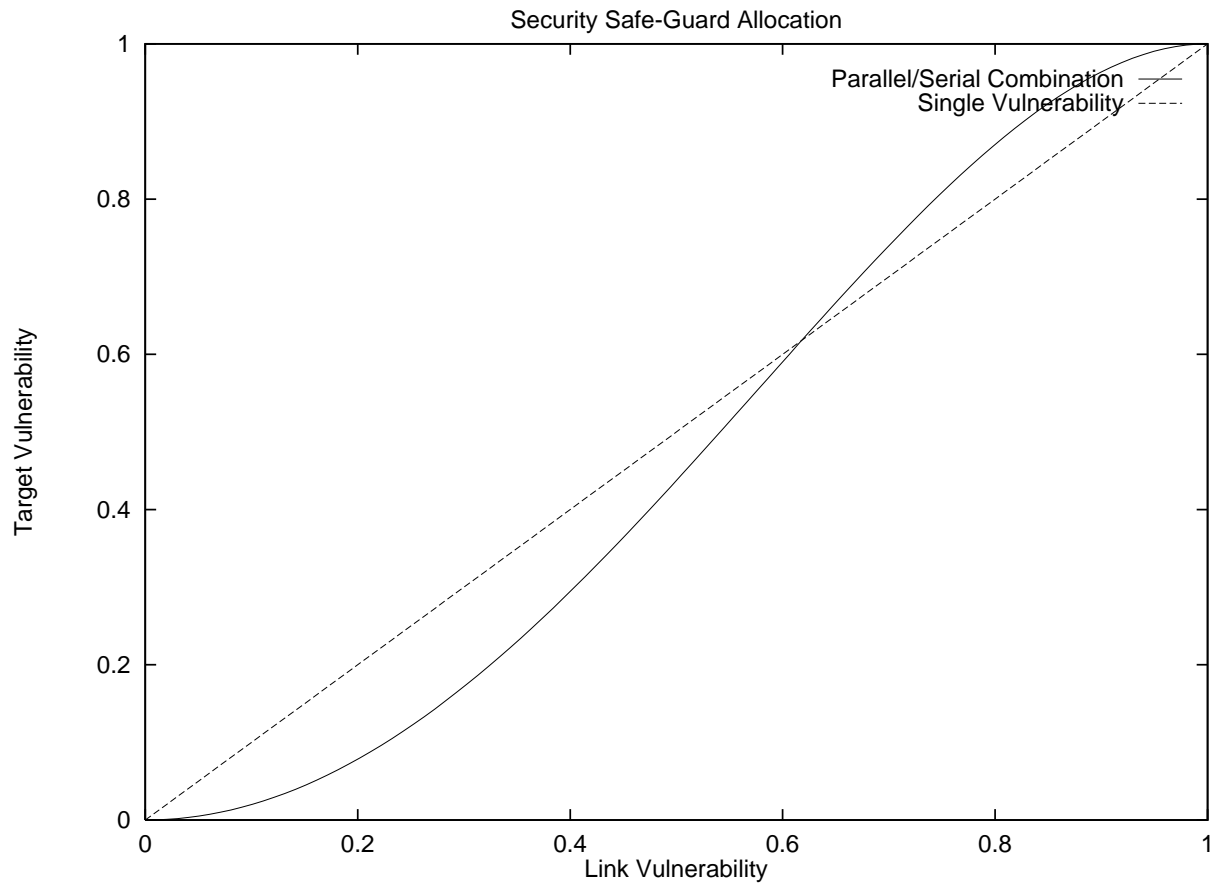


Fig. 3. Effect on Vulnerability of Security Safe-Guard Allocation.

IV. OPTIMAL SECURITY SAFE-GUARD ALLOCATION

Current network safe-guards are usually in the form of firewalls, that is, a hard shell around the network, while the network itself is easily penetrable. With the Network Insecurity Path Assessment Tool, the impact of other types of safe-guards and their allocation can be determined including Active Network-based security safe-guard strategies.

V. OPTIMAL CONTROL AND STRATEGY

As an attack takes place, the defender will use Network Insecurity Path Assessment Tool to study the effectiveness of various strategies using actual network vulnerabilities, but within the safety of a simulation environment. The optimal location of services to be cut will be determined using the Network Insecurity Path Assessment Tool analysis tool. The effect of concentrating on reducing specific vulnerability classes will be the focus, rather than cutting-off access to entire network hosts that have been compromised. Also, by studying the past history of an attack, it will become apparent which vulnerability classes a particular attacker prefers to exploit.

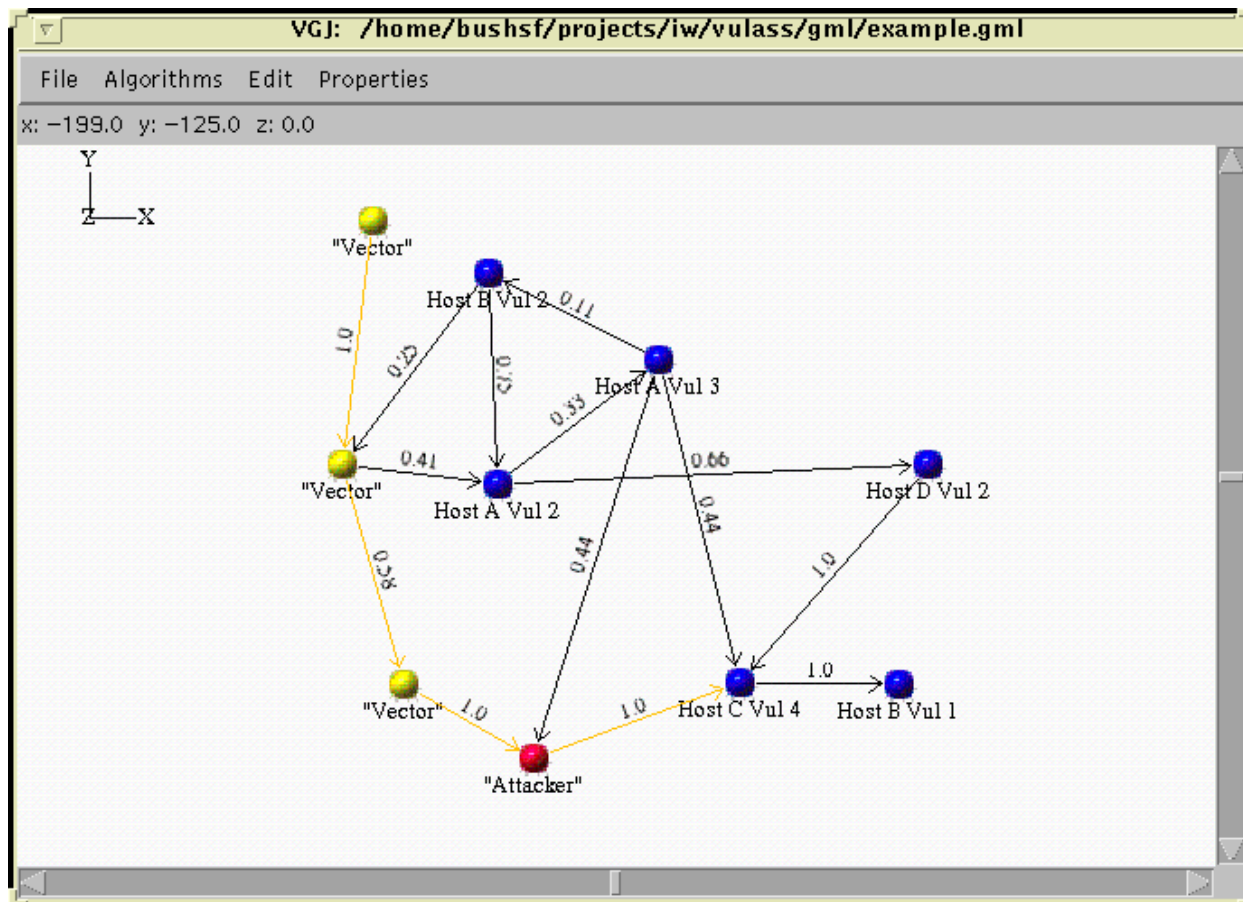


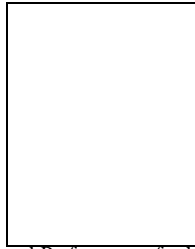
Fig. 4. An Example of an Attack in Progress.

APPENDIX

I. JAVA DOCUMENTATION

REFERENCES

- [1] Stephen F. Bush and Bruce Barnett, "A Security Vulnerability Assessment Technique and Model," Tech. Rep. 98CRD028, General Electric Corporate Research and Development Center, Jan. 1998.



Stephen F. Bush Stephen F. Bush is a Computer Scientist at General Electric Research and Development (GE CR & D) in Niskayuna, NY. Steve is currently the Principal Investigator for the DARPA funded Active Networks Project at GE. Before joining GE CR & D, Stephen was a researcher at the Information and Telecommunications Technologies Center (ITTC) at the University of Kansas where he contributed to the DARPA Rapidly Deployable Radio Networks Project. He received his B.S. in Electrical and Computer Engineering from Carnegie Mellon University and M.S. in Computer Science from Cleveland State University. He has worked many years for industry in the areas of computer integrated manufacturing and factory automation and control. Steve received the award of Achievement for Professional Initiative and Performance for his work as Technical Project Leader at GE Information Systems in the areas of network management and control while pursuing his Ph.D. at Case Western Reserve University. Steve completed his Ph.D. research at the University of Kansas where he received a Strobel Scholarship Award. He can be reached at bushsf@crd.ge.com and <http://www.crd.ge.com/people/bush>.