LBL-38670
UC-400

Lawrence Berkeley Laboratory
UNIVERSITY OF CALIFORNIA

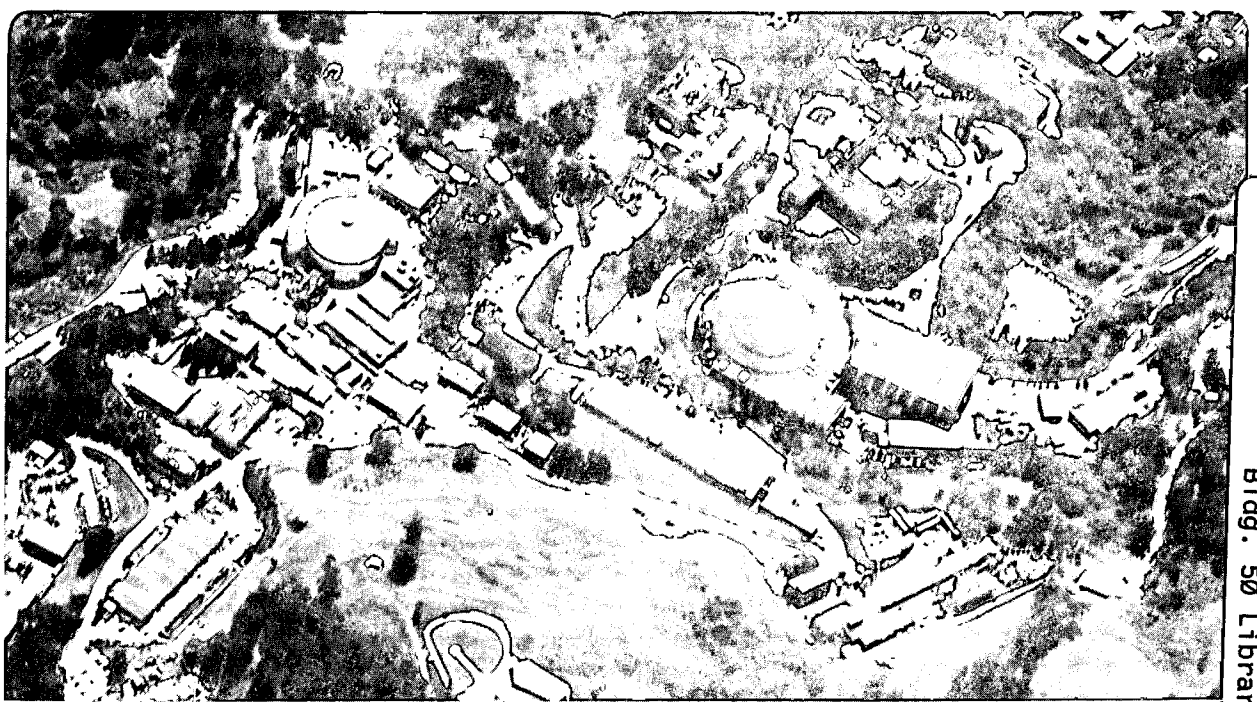
Information and Computing Sciences Division

Presented at the *Internet Security Workshop*,
Haystack Observatory, MA, May 20–21, 1996,
and to be published in the Proceedings

Evaluating Network Security: Performance-Based Measures of Effectiveness

D.F. Stevens

April 1996



Prepared for the U.S. Department of Energy under Contract Number DE-AC03-76SF00098

DISCLAIMER

LBL-38670
UC-400

Evaluating Network Security: Performance-Based Measures of Effectiveness

David F. Stevens

Information and Computing Sciences Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California
Berkeley, California 94720

April 1996

Prepared for the
Internet Security Workshop
Haystack Observatory, Massachusetts
May 20-21, 1996

This work was supported by the Director, Office of Energy Research, Office of Basic Energy Sciences, of the U.S. Department of Energy under Contract No. DE-AC03-76SF00098.

Evaluating Network Security: Performance-based Measures of Effectiveness*

D. F. Stevens
Ernest Orlando Lawrence Berkeley National Laboratory
Berkeley, CA 94720

Position: The Federal Internet community should adopt *performance-based* measures rather than *administrative compliance* measures for the evaluation of computer and network security.

Rationale: Because many of the possible performance measures of security are inherently difficult to make, validate, and interpret, they have often—perhaps usually—been supplanted by administrative compliance measures. Although these latter have some justification in a presumed correlation between the administrative procedures involved and an increased level of security, many of them have been in place for so long that the procedures have become ends in themselves: procedure has become more important than performance and their value as security mechanisms has become irrelevant. For example, the evaluation of formal incident response procedures can consume more resources than analysis of the actual incidents.

Definitions

1. A *performance-based measure* is one that is based on the results obtained, not on the method used to obtain those results or on the quality or completeness of the documentation. Examples of performance-based measures that might be employed in computer and network security include the number of incidents detected, the amount of data lost or compromised, the cost of protection.

2. An *administrative compliance measure* is one that is based on adherence to formal procedures and evaluation of the documentation that accompanies the procedures. Example of administrative compliance measures that might be employed in computer and network security include the existence and "completeness" of a formal computer protection plan, formal certification and accreditation documents, and formal corrective action plans.

Note: Most of the performance-based measures are quantitative in nature (*how much* and *how many*), whereas most of the administrative compliance measures center on the existence of documentation in a prescribed format. It should not be thought, however, that all quantitative measures are necessity performance-based.

The case against administrative compliance measures

Administrative compliance measures are ineffective, costly, and diversionary. By "ineffective" I do not mean that they fail to improve the quantity of documentation produced, but that there is

* This work was supported by the U. S. Department of Energy under contract No. DE-AC03-76SF00098.

little causative correlation between a site's score on administrative compliance and its ability to prevent and detect damage to, and compromise of, its information. Configuration plans, organization charts, incident reporting procedures, and audit trails do not protect information.

Administrative compliance measures are labor-intensive. They involve the time-consuming creation and maintenance of detailed documentation of rapidly changing systems. They also encourage the detailed examination of documentation and procedure by small armies of assessors and auditors, resources that might be better employed in assessing (or even increasing) the security of the systems rather than the completeness of the surrounding paperwork.

Administrative compliance measures are diversionary; they divert both attention and resources away from the real problem. The emphasis in many formal security procedures appears to be more concerned with placing the blame when an incident or breach occurs than on either preventing or recovering from the problem. Finally, the widespread use of these processes has caused them to be perceived by many administrators as major contributors to computer and network security, often to the extent that no performance-based measures are employed.

Performance-based evaluation

Computer and network security offer a number of possibilities for performance-based measurement, but the measures are generally indirect, incomplete, or *post hoc*. Nevertheless, they provide some insight into the level of protection that actually exists at the site. Brief descriptions of several possibilities are given below. This is not an exhaustive list, and the intent is not to propose a specific selection, but to inspire more in-depth consideration of true performance-based measures.

- *time to detection*: the time from commission of a break-in of some sort until it is detected by the system or staff of the site. This is a particularly important aspect of protection against fast-spreading corruption of any kind, including viruses and password collection.

- *number detected*: an indication of the amount of hostile activity and the sensitivity of the detection mechanism. This is obviously less useful as a measure of the quality of the system than the *fraction* of attacks detected would be, but that would require a trustworthy count of undetected attacks, a count that is difficult to obtain.

- *fraction self-detected*: that fraction of all known attacks on a site or from a site that are detected by the site itself.

- *dollars lost* (as a percentage of loss potential): the cost borne by a site in coping with an attack. This includes repairing the breach, installing new locks (although this could involve some double counting; see the next measure), repairing the damage, restoring the data, identifying the problem, re-authenticating the users, etc. In a commercial enterprise, it could also include substantial indirect costs such as loss of market share or loss of customer—or public—faith.

Note that this is a relative measure. A million-dollar loss might be sustainable if it occurred because all a site's resources were dedicated to closing a billion-dollar hole.

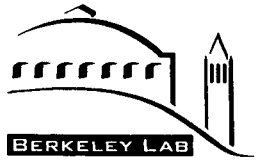
- *dollars spent for security* (as a percentage of loss potential): another relative measure that addresses the cost-effectiveness of a computer and network security program. This should include all costs incurred by the entire using community, not just the costs of the formal tools and the computer security professionals. These costs are often underestimated or overlooked. The cost of simple password protection in lost time at login amounts to approximately 1 FTE for every thousand users (2 seconds per password, and an average of 3 logins per working day). That doesn't sound like much, but it is rarely—if ever—considered explicitly, and in any case is only a portion of the cost; it doesn't include the cost of administering the password policy (checking for guessable passwords, for example, or password aging), the frustrations involved in recovering from a lost or forgotten password, or the great loss of protection when a system saddles a user with a password that is not memorable.

- *known countermeasures installed*: the fraction of systems at a site that have implemented countermeasures against known vulnerabilities in installed software. While this is an absolute measure, it should be used in conjunction with a combined cost and threat analysis.

- *"white hat" inspection*: this is not a measure, *per se*, but a method that can be useful in carrying out a performance-based evaluation. It consists of a concerted attack conducted by a trusted adversary, followed by a frank discussion of vulnerabilities found.

Summary

Performance-based evaluation of computer and network security is possible. It is necessary if we are to achieve true network security. It should not be avoided simply because it is more difficult than evaluation based upon administrative compliance.



ERNEST ORLANDO LAWRENCE BERKELEY NATIONAL LABORATORY
TECHNICAL AND ELECTRONIC INFORMATION DEPARTMENT
UNIVERSITY OF CALIFORNIA | BERKELEY, CALIFORNIA 94720