Title
Promoting a Healthy Skepticism with Regard to Information Processing

Author
Stevens, D.F.

Publication Date
1991

LBL-30110

Lawrence Berkeley Laboratory
UNIVERSITY OF CALIFORNIA

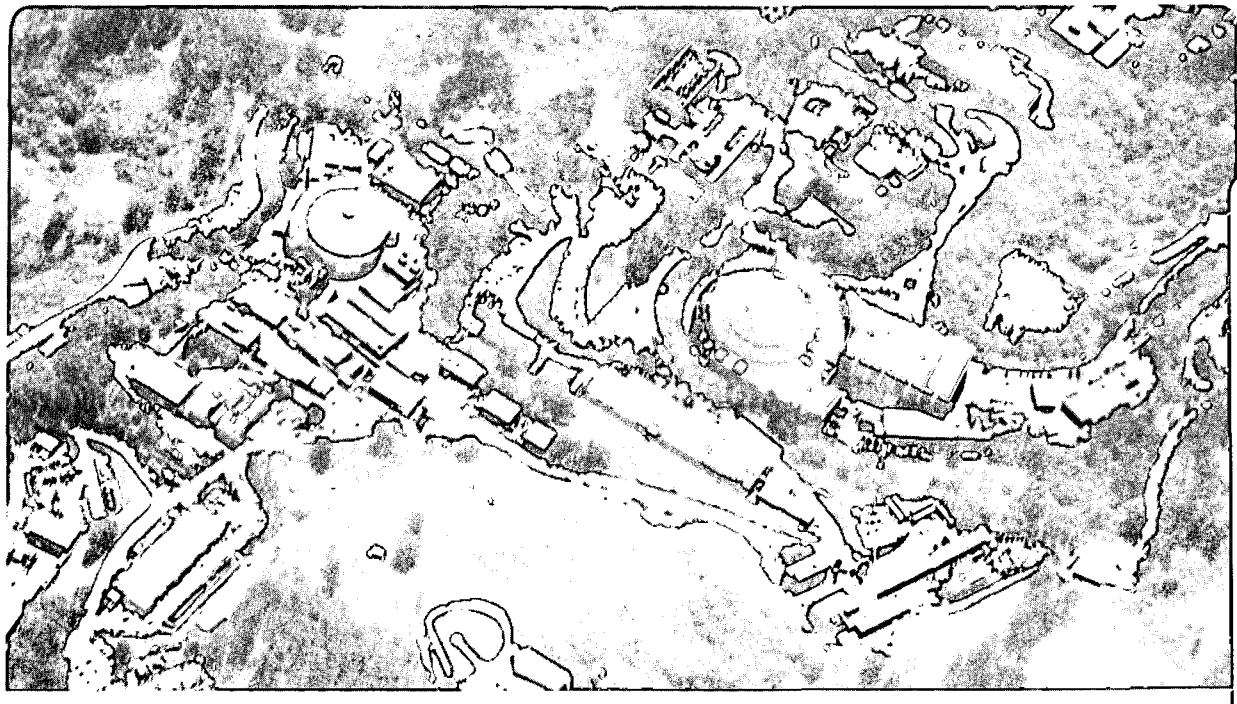
Information and Computing Sciences Division

To be presented at the Seventh International Conference and Exhibition on Information Security: Creating Confidence in Information Processing, Brighton, England, May 15–17, 1991, and to be published in the Proceedings

Promoting a Healthy Skepticism with Regard to Information Processing

D.F. Stevens

January 1991



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

DISCLAIMER

Promoting a healthy skepticism with regard to information processing*

(The development of a computer security program for a collaborative research environment)

David F. Stevens
Information and Computing Sciences Division
Lawrence Berkeley Laboratory
1 Cyclotron Road
Berkeley, California 94720

January, 1991

Prepared for
The Seventh International Conference and Exhibition
on Information Security:
Creating Confidence in Information Processing

Brighton, UK, 15-17 May, 1991

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

Promoting a healthy skepticism with regard to information processing*

(The development of a computer security program for a collaborative research environment)

David F. Stevens
Lawrence Berkeley Laboratory
1 Cyclotron Road
Berkeley, California 94720, USA

ABSTRACT

Computer security professionals and members of collaborative research environments have conflicting objectives with respect to computer and network access, and different understandings of what constitutes a "reasonable" organization. These differences create tension between the two communities and make the achievement of an acceptable level of security a matter of some difficulty in such environments. We consider some of the differences and present the elements of a program aimed at promoting sensible computer and network security in the research milieu.

1. Introduction

Implicit in the theme of this conference is the notion that people do not trust Information Processing, and that their lack of confidence can be overcome by improving the security and reliability of the systems they use. This is certainly consonant with the public view of information processing as conveyed in the popular press and reinforced by a wealth of anecdotal evidence, but there are communities of users in which there is insufficient *dis*trust of Information Processing, in the sense that a strong desire for worldwide connectivity overrides any reservations they may have about the possible negative consequences of poor security. International collaborative research environments typically are such communities. They have enthusiastically embraced the technology that has enabled them to communicate so easily with their peers, and are reluctant to see the dangers implicit in free access.

Because of their rather casual attitudes towards data protection, their distrust of and resistance to centralized authority and responsibility, and their very strong desire for full connectivity, they tend to appear to be actively inimical to a traditional approach to computer and network security. It should be understood that their resistance is not born of antagonism so much as of a different view of the world of information, and of the proper place in that world for "security".

2. Cultures in Conflict

The characteristic research environment today consists of personal workstations networked locally to each other and to various servers, with further direct or indirect connections to national and

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

international networks. Each scientist is essentially autonomous, acting as his own system manager, and free to join a large number of research communities that collectively embody a wide range of formality, coherence, and observance of sound security practice. Such central policies as exist, do so by consent rather than by decree. To the scientist, "the Network" is the sum of all the communities to which he belongs. Within this extended "Network" there is no overall authority, no common set of security precautions, and not even a general agreement about which aspects of security are properly the responsibility of "the Network" and which are the responsibility of the individual nodes. Few of the users have more than the most rudimentary knowledge of the topology of the connecting infrastructure, or where the responsibility for its administration lies. They have little knowledge of where the responsibility for security lies within any node other than their own. There is no generally recognized point of contact for the dissemination of information about attempted penetrations. In sum, the research scientist treats "the Network" much as he would the telephone system, as a medium of communication about which he needs to know nothing except how to address his colleagues.

The computer security professional cannot take this black-box approach to "the Network". He must know both the physical and administrative topologies: the nodes and connections, and the Authorities in charge of each, and his inability to do so is a source of great frustration. Instead of rejoicing at the breadth of possible connections, he worries about the number of unknown "users" who have access to the many gateways into his domain.

These, and other, considerations give rise to two cultures that differ in many fundamental ways. While these differences need not lead to overt conflict, they are bound to create significant tension. We list here a few of the many examples of the differing viewpoints that contribute to this tension.

- The research community tends to be oblivious to the possibility that any of their data or systems might be the targets of annoying or malicious penetration attempts. They have no secrets, and so they believe they are not worth attacking; they assume that all persons with network access will always act ethically, correctly, helpfully, and harmlessly. Computer security professionals know that all systems are under more or less constant attack, simply because they are there, and the attackers are capable of inflicting both accidental and deliberate damage.
- Collaborative research environments are collegial. They are loose confederations, spread over many organizations, often in several countries, and there is no single chain of responsibility or command. There is no common authority to whom all the participants in a collaborative research environment report. By contrast, the organizations that develop traditional computer security procedures are strongly hierarchical, and the procedures they produce assume the existence of a single, *strong* chain of command. Traditional security organizations do not understand the collegial style, and their procedures cannot cope with it.
- Collaborative research environments are characterized by a lack of routine. Researchers are free, within broad limits, to establish their own procedures, and to change them essentially instantaneously to take advantage of new insights, new equipment, new technology, and the talents of new personnel. Standard security practice, on the other hand, is designed to force

operations to be routine, and to remove freedom and discretion from the manner in which they are performed.

- Collaborative research environments are designed to facilitate connectivity, the sharing of knowledge among all the members, and the cross-pollinization of ideas throughout the whole domain of enquiry. By contrast, traditional security measures include the principle of *division of responsibility*, which partitions each domain into single-function regions and erects impenetrable fences between them.
- Policy and practice in collaborative research environments are generally aimed at maintaining and increasing access, to the broadest posible extent. Traditional computer security is founded on a basic distrust of everyone not known, validated, and authenticated to/by the system, and is aimed at restricting access to the narrowest possible population.
- Collaborative research often involves the presence at a site of a constant flow of visiting workers, whose time on the spot is brief and whose need to share information is great. The imposition of even relatively simple security precautions, such as the prohibition of password-sharing, or the elimination of any password or system ID known to a departed visitor, can place a significant procedural burden on the stable core of the group. On the other hand, failure to observe these precautions can make the achievement of even a minimally acceptable level of security impossible.

3. Reconciling the Worlds of Security and Research

The problem in a nutshell is to allow unlimited connectivity while providing adequate security. For this to be accomplished, both the researchers and the security professionals are going to have to modify their accustomed ways of doing things to some extent. If this is to be done without a full-scale clash of cultures, the initial adjustment must come from the security establishment, primarily because, whereas connectivity *can* be achieved without security or the cooperation of the security professionals, security cannot be achieved without the cooperation of the research community. The research community contains many extremely creative people whose culture is to view constraints—whether natural or administrative—as challenges to be overcome rather than as limits within which to work. An unthinking traditional approach to security is more likely to motivate them to circumvention than to observance. On the other hand, if the research community can be convinced that a modicum of security is in their best interest, they will turn their creative energies to supporting security instead of subverting it.

How, then, can their cooperation can best be achieved? By establishing a security program that is designed for the milieu in which it is set. Such a program cannot depend upon rigid enforcement of centrally-imposed rules, but must distribute responsibility for security in the same manner that responsibility for the quality of the research is distributed. It must recognize a realistic span of control. It must admit of the existence of multiple domains with differing requirements, but with the need to communicate with each other. It must assume a reluctant population, and minimize the burden that accompanies the implementation of the security program. It must provide each user

with the knowledge and the tools necessary to maintain adequate security. It must make it simple to install and use elementary precautions. It must make it difficult or awkward to maintain known security flaws.

The conference theme suggests that trusted *systems* are the highest form of the security practitioner's art; I suggest rather that even trusted systems depend upon proper operation by people, and that a successful program in the collaborative research environment must depend upon trusted *people*. The irony is that to create a suitably trustworthy user population for maintaining network security we must convince them to view the rest of the world with a healthy *mis*trust.

4. Elements of a Program

The program outlined here is founded on the principle that responsibility for security belongs to everyone who has a network connection. In the case of a general collaborative research environment, that includes essentially every professional, administrative, clerical, and managerial employee. The program has been developed over a period of several years, drawing on a number of sources. The primary ones are U. S. Department of Energy Order 1360.2A, which specifies the functional elements of an acceptable program, but allows individual installations to define specific implementations that are well suited to their own situations; a set of risk analyses; and a network security policy developed by an institution-wide task group. (More detail on the actual policies is provided in the appendix.) In summary form, the program:

- provides constant small doses of security awareness raising.
- assigns to each node responsibility for the results of actions originating from the node, and gives each node the authority to refuse traffic from a node it considers to be untrustworthy.
- incorporates risk analyses to determine the level of protection required.
- provides constant small doses of security awareness raising.
- offers access protection in the most direct manner (via passwords), but includes password checking and aging.
- requires the monitoring of network connections to detect and investigate unauthorized access attempts.
- provides constant small doses of security awareness raising, supplemented with periodic discussions of ethical network behavior.
- provides assistance in the identification of sensitive applications.
- places significant emphasis on the development of a comprehensive incident-handling procedure.
- provides constant small doses of security awareness raising.

The most important piece of this program is steps 1, 4, 7, and 10, for it is largely through these periodic dosages that the research community has become convinced that good security practice is necessary. It is unfortunate that some of these doses have involved loss of data, either for our own

scientists or for their colleagues in other laboratories and universities. (To paraphrase Ben Franklin: Experience keeps a dear school, but scientists will learn in no other.) It has also been useful to show them how often their passwords—or those of respected colleagues—can be decoded if they are not chosen in an intelligent fashion. Several other, relatively standard, mechanisms are also in use: Newsletter articles, with reminders of problems, virus warnings, and the like; reports to and through various representative committees; policy memos that are updated and reissued annually; security awareness modules in all computer-oriented classes; and a packet of computer-security-awareness material for new employees. We also take advantage of highly publicized events, such as Stoll's *Cuckoo's Egg* caper and the Internet worm of November, 1988, to remind the scientists that they are, truly, at risk.

We have found that it is possible to heighten the understanding and awareness of the research community, and to sensitize them to the threats to the integrity of their data that can arise from unlimited and uncontrolled access to computer networks. Despite their tendency to assume they are immune to some worldly cares, and hence to security, they *can* be taught a healthy skepticism that results in a reasonable level of good practice.

Appendix: Provisions of a sample network security policy

A. General Policy

The Laboratory's computer systems and all sensitive unclassified information contained therein shall be protected from improper use, alteration, manipulation, or unauthorized disclosure. Failure to observe proper computer and network security practices may result in a reduction of computer and/or network access privileges.

B. Responsibilities

- The Laboratory Computer Protection Program Manager (CPPM) is responsible for defining, implementing, and administering the Laboratory's computer security program.
- Division Directors are responsible for assuring that Laboratory computer security policies and procedures are observed within their Divisions.
- Supervisors and managers are responsible for ensuring that employees under their supervison maintain a continuing awareness of proper computer security practice. (A standard computer security awareness statement is appended.)
- System Managers are responsible for maintaining an appropriate level of security for their systems, and for responding appropriately to the detection of a security incident. They have the authority to deny access to their systems to any person observed not using proper computer security practice. (Further details on System Manager responsibilities are given below.)
- Network Managers are responsible for maintaining an appropriate level of security for their networks, for knowing how to isolate their networks from all non-Laboratory connections, and for responding appropriately to the detection of a security incident. They must authorize and register all connections to their networks. They have the authority to deny network access to any system or external connection for security reasons.
- Individual users are responsible for knowing and observing Laboratory computer and network security policies, and for bringing any security violations to the attention of their System Manager, the Laboratory CPPM, or other proper authority.
- The Protective Services Department is responsible for maintaining a 24-hour telephone service to assist users to locate appropriate management or administrative authority to deal with a suspected data security incident.

C. System Managers

1. Designation of a System Manager

Every system connected to the Laboratory network must have a designated System Manager who is responsible for maintaining proper controls over the use of the system. "Proper controls" are construed to be those appropriate for the nature of the system, the security tools it provides, and the sensitivity of the data it contains.

2. Login ID

Login ID's are to be issued by System Managers or their designees, who shall maintain records of the names and current addresses of all active users. Each login ID is issued to an individual. Group login ID's are not permitted. The individual to whom the ID is issued is responsible for all activity that takes place under that login ID.

3. Passwords and password protection

All access is to be protected by passwords that conform to the following rules:

- Default passwords (i.e., those distributed with the system) are to be changed before the system is made available to users.
- Password cannot be the same as the login ID.
- Password must be at least 6 characters long.
- Password cannot consist solely of a repeated single character.
- Password should be chosen so that neither login ID nor user name provide a clue to the password.
- Password cannot be a dictionary word or common name.
- Passwords are not to be written into files or electronic mail.
- Passwords and login ID's are not to be associated in clear text in any context.
- Passwords are not to be shared.
- Changes of password cannot equal the previous password.

4. Expiration of passwords and login ID's

Passwords and ID's are to be expired in accordance with the following schedules:

- The initial password issued to a new user is a single-use password; it must be changed the first time the user uses the system.
- Passwords expire within 180 days of definition.
- An initial login ID is deactivated after 10 days of non-use.
- Login ID's are deactivated after 90 days of inactivity.
- Files associated with inactive login ID's are archived 30 days after the login is deactivated.

5. System safeguards

The safeguards that are provided by the operating system in use should be invoked to the maximum extent that does not interfere with the work of the users. These include:

- Control over system privileges.
- Protection of the password file.
- User notification of unsuccessful login attempts.
- Temporary deactivation of login after several successive failures.
- Installation of alarms on sensitive files.
- Encryption of sensitive information.
- Less-than-universal defaults for file access.

6. Network access

- Scripts may not contain network access passwords.
- Use of the default DECnet account is not permitted.
- Tymnet access requires the use of Divisional accounts and passwords.
- Use *proxy* access for remote logins to VMS systems.
- *unix .rhost* entries should be aged and expired after 180 days.

7. Physical security

Physical access to all Laboratory computers shall be limited to authorized personnel.

D. Basic Procedure for Handling Computer and Network Security Incidents

An employee who encounters a suspected computer or network security incident (attempted unauthorized access, or the occurrence of a virus or worm) should first try to inform the appropriate people (by telephone, not E-mail), and then, if necessary, respond to the threat.

To inform the appropriate people, call one of the following, and report the system affected and the nature of the problem.

- If you are using a multi-user system, call your system manager; if you are using a single-user workstation, call the appropriate technical support group.
- The Computer Protection Program Manager (CPPM).
- The Divison Director for Computation.
- The Protective Services Department. (They have a telephone tree to assist them to locate an appropriate person.) Be sure to specify that you are calling to report a *data security incident* in progress.

To respond to the threat, the following general rules apply.

- In all cases: Log the incident and inform the appropriate personnel.

- In an isolated case of unsuccessful attempt at entry (i.e., a single, unrepeated, unsuccessful attempt): No further action is necessary unless and until the attempt is repeated.
- In the case of a successful penetration, where it appears that the integrity of user data is threatened: Attempt simple close-out; that is, shut down the known access paths. Monitor all accounts that the attacker is known to have corrupted.
- In the case of discovery of a rogue program: Isolate your system and quarrantine all disks and tapes that have been on your system since the introduction of the rogue program. *Do not connect to any other system or transfer any programs or data from your system to any other system until your System Manager has declared your system to be clean.*
- In other cases: Confer with Division management and/or the CPPM.
- In the absence of other advice or information, act to protect the data rather than to monitor or trap the attacker.

E. Confidentiality of Computer Files

Computer files are accessible only by the person responsible for those files unless that person has explicitly authorized others to access them. In particular, browsing is not permitted. ("Browsing" is unauthorized reading of directories or files not belonging to the browser. The scanning of public files such as telephone lists, stores catalogs, help files, etc., by users is not considered to be browsing.)

This policy applies regardless of the level of access protection assigned to a particular file.

In the course of their work, certain authorized individuals, such as system managers and computer security personnel, are required to inspect users' files. Under no circumstances, except as specified below, are the contents of those files to be revealed, and then only to the Laboratory Computer Protection Program Manager, the Division Director for Computation, or such other persons as the Director may specify. In the following instances the indicated information (and only that) may be divulged:

- evidence of unauthorized access, internal or external;
- evidence of improper use of Laboratory facilities;
- evidence of security-threatening practices.

F. Computer Security Monitoring

To ensure adequate security of Laboratory computer systems and networks, a program of computer security monitoring will be conducted under the supervision of the Laboratory Computer Protection Program Manager (CPPM). It will include the following activities, as necessary:

- annual inventory of sensitive applications
- random sampling of user files
- verification of proper control and authentication of new users

- verification of proper password procedures and use
- verification of proper physical security
- monitoring of network traffic
- monitoring of usage patterns

Any apparent violation of Laboratory policy, attempt at unauthorized access, or any situation that exhibits less than acceptable computer security, will be reported to the CPPM for further action.

In all cases involving the monitoring of user files and data traffic, Laboratory policy on confidentiality of computer files applies.

G. Guidelines

Guidelines on the following topics are available from the CPPM:

- Access Protection
- File Protection
- Development of Sensitive Unclassified Applications
- Risk Analyses
- Contingency Plans

H. A Sample Security Awareness Statement

Note: These rules do not replace formal Laboratory computer security policy as enunciated in the applicable Policy and Procedure Memos and in the Regulations and Procedure Manual. They are intended to be a periodic reminder that computer security is the responsibility of everyone at Laboratory who uses computers.

These rules apply to all Laboratory computer users, regardless of the size or location of the computer system involved.

1) All employees share in the responsibility to protect the Laboratory's information assets and resources.

2) Do not keep any password in a public place. "Public place" includes written on a chalkboard, taped to a terminal, written in a file to which any other person has access, or any other location that would render accidental disclosure likely.

3) Do not share your password with anyone.

4) Do not read -- or browse through -- files for which you have no authorized access.

5) Do not use Laboratory computers for personal (or any other unauthorized) purposes.

6) Do not make or use unauthorized copies of any software.

7) Do not load or use any software from a source not known to be reliable. Public bulletin boards are not reliable sources.

8) Observe all system-specific computer security policies and procedures established by the System Manager of any system you use.

9) If you have reason to suspect an unauthorized access on any system, contact the System Manager or the Laboratory Protective Services Department.

10) If you have any questions about these rules, or any computer security matter, contact your supervisor, the System Manager of the system involved, or the Computer Protection Program Manager.

I have read and understand the foregoing computer security rules.

_____

(signature) (date)

LAWRENCE BERKELEY LABORATORY
UNIVERSITY OF CALIFORNIA
INFORMATION RESOURCES DEPARTMENT
BERKELEY, CALIFORNIA 94720