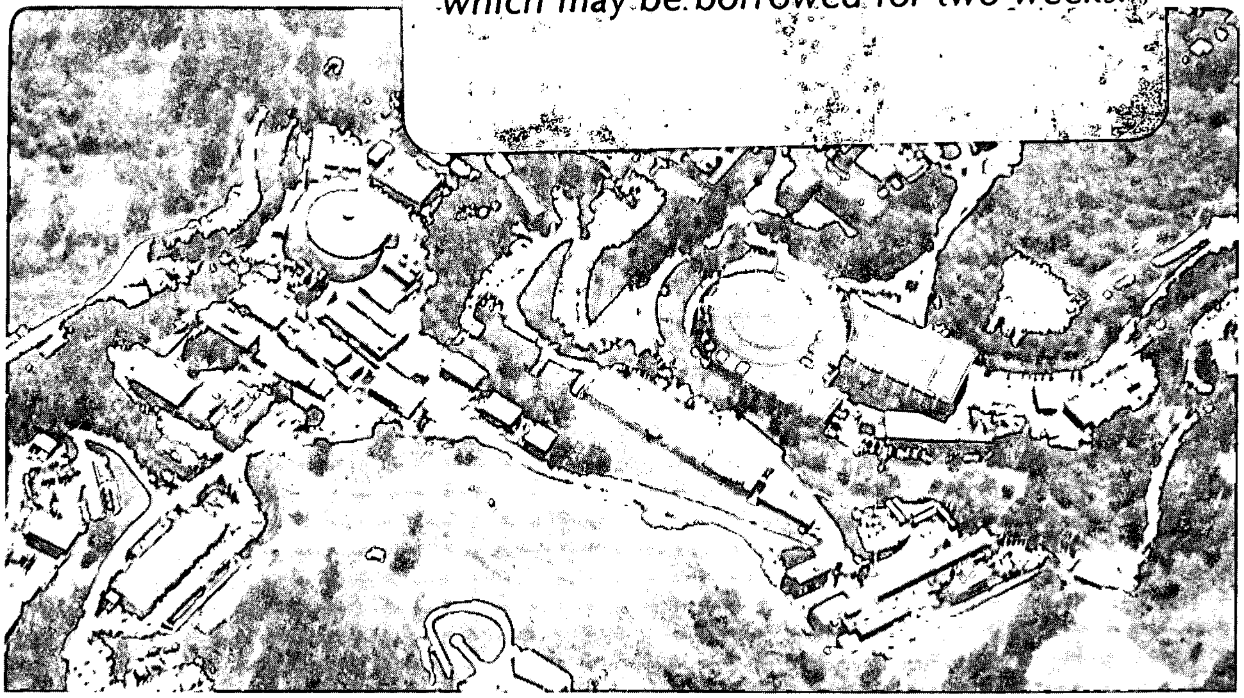
Lawrence Berkeley Laboratory
UNIVERSITY OF CALIFORNIA, BERKELEY

Information and Computing Sciences Division

RECOMMENDATIONS FOR SECURITY POLICY FOR ALL NETWORKED COMPUTERS AT LBL

M. Atchley, E. Beals, D. Cleveland,
T. Hitchcock, W. Jaquith, R. Kerth,
B. Nordman, J. Noring, D. Stevens,
C. Stoll, E. Sheena, and D. VanZile

April 1987



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

DISCLAIMER

This document was prepared as an account of work sponsored by the United States Government. While this document is believed to contain correct information, neither the United States Government nor any agency thereof, nor the Regents of the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by its trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or the Regents of the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof or the Regents of the University of California.

LBL-23303

Recommendations for Security Policy for All Networked Computers at LBL

Marv Atchley, Eric Beals, Dave Cleveland, Tom Hitchcock,
Wm. Jaquith, Roy Kerth, Bruce Nordman, John Noring, Dave Stevens,
Cliff Stoll, Ed Sheena, Dan VanZile

Computer Security TPEG Committee
Information and Computing Sciences Division
Lawrence Berkeley Laboratory
University of California
Berkeley, California 94720

April 1987

This work was supported by the U.S. Department of Energy under Contract DE-AC03-76SF00098.

RECOMMENDATIONS FOR SECURITY POLICY FOR ALL NETWORKED COMPUTERS AT LBL

Computer Security TPEG Committee

Marv Atchley, Eric Beals, Dave Cleveland, Tom Hitchcock,
Wm. Jaquith, Roy Kerth, Bruce Nordman, John Noring, Dave Stevens,
Cliff Stoll, Ed Sheena, Dan VanZile

April 15, 1987

Charge: What should we do to improve security?

Our goal is to establish and maintain computer security policies that satisfy both the law and common sense without imposing undue restrictions that may interfere with the LBL mission. We must accomplish this in an environment that is unique to DOE - a major multi-purpose research laboratory that is adjacent to a major university, and whose staff includes researchers and students.

Scope:

The security policy discussed by this committee is intended to cover all on-site mainframes and workstations that are networked via the LBL Ethernet or by dedicated lines.

DOE Unclassified Computer Security Policy (1360.2)

It is DOE policy that DOE computer systems and sensitive unclassified information be protected from improper use, manipulation, or unauthorized disclosure as a result of criminal, fraudulent, or other improper actions.

Summary:

The committee believes that the security policies adopted by Computing Services are appropriate for LBL, and recommends implementing them on all LBL networked computers.

We also recommend that Computing Services monitor all of these machines for compliance to the policy.

Threats to LBL computing:

- unauthorized access to and divulging of research data.
- unauthorized access to and divulging of personal data.
- destruction or modification of data or programs.
- unauthorized use or copying of proprietary software.
- unauthorized use of computer systems.
- denial of service to users by system disruption.
- use of LBL as a conduit for network hackers.
- physical damage or destruction of hardware.

A real threat to scientific computing is the possibility of onerous government regulations that could be imposed by a Government agency if it was perceived that we are not protecting the public's interest. Such regulations are possible following a media over-reaction to a computer hacking incident that was the result of lax security practices.

The Unauthorized User

The most serious threat to our computer systems is caused by unauthorized users. Unauthorized use is gained in the following ways:

- **guessing password**
  This is possible on any system where users are allowed to choose their own password. On the Computing Services machines, a password checker is run weekly. It detects default passwords (password=login), and also detects passwords which are a subset of the login. Passwords that fail this test cause the login to be disabled. Our systems also require a minimum 6-character password, which decreases the likelihood that anyone would guess them.

  Although most systems don't permit significant repeated attempts at password matching against a dictionary by another computer, the use of words found in the dictionary is risky.

  Complex, yet easily-remembered passwords can be achieved by teaching users a few tricks: including a special character or combining more than one short word into a password.

- **stealing password**
  Passwords can be stolen if written down. The necessity of writing down passwords is minimized by allowing users to choose something they can easily remember.

  Logins and Passwords have been stored in on-line files for ease of access to other machines. We have observed an incident where a hacker scanned user files in a computer on the LBL network, and and found a login and password which was then used to break into another computer.

  We are opposed to the use of machine-generated passwords. Our desired level of security does not require them. We also believe they are often self-defeating because the difficulty of remembering them causes people to write them down.

  It is very unlikely, although possible, that someone could steal a password by observing the person type it in.

- **receiving password** (as a gift)
  Computer security has not been regarded seriously by many persons, and passwords have been given to family and friends to allow casual inspection and training. Although not normally a serious breach of security, the possibility exists for misuse, and it fosters a lax attitude about the problem. Some teenagers consider knowledge of a password as a (negotiable) status symbol.

  We have detected misuse of computer systems at LBL when a group of students shared the same login and password. As there seemed to be no specific responsibility for the account, the password was given to other students, who used the machines for game-playing.

  From Gary Jensen, NCAR: "Treat your password like your toothbrush: Change it once in a while, and don't pass it around."

- **Failure to Implement Password System**
  Some research machines that are on the network have not implemented password systems because of the perceived inconvenience.

- **bypassing password system**
  A system bug in UNIX4.2BSD allowed knowledgeable users to bypass the password system. This has been fixed. There is no known way to bypass the VMS password system.

- **Guest Accounts with trivial passwords**
  Formerly, it was common practice to allow guest accounts on computer center machines. Although this allowed visiting researchers quick access for test purposes, it also allowed easy access to hackers.

- **Maintenance Accounts**
  Operating systems, such as VMS, are distributed for installation with a common login and password for the DEC maintenance engineers. Unless changed promptly by the system

manager, this can be a serious breach - this login brings with it a very high level of system privileges.

Late Bulletin: As of March 9, 1987, DEC no longer follows the above practice. DEC will not distribute new systems with a "Maint" login, nor will they be responsible for that "Maint" login after they leave the site. They will assume that the login is created and deleted for each of their sessions.

o **Network Access**
Networks have proven to be a threat by providing access to long-distance hackers, who do so at little risk of trace-back. Note that almost any student at any college or university in the western world has access to the LBL network.

The threat from networks such as TYMNET can be minimized by effective use and management of their password scheme.

o **Dialin Access**
The common availability of personal computers and modems has created an army of potential hackers. The phone numbers for our Develcon dial-in modems have been printed in a national hackers magazine.

Various techniques for achieving higher levels of dial-in security are available. Most notable are systems that only allow connection after dial-back to approved phone numbers, and passwording of the answering modems or the terminal switch.

The level of security afforded by a properly-managed password checker at the host system level is adequate for LBL computer systems. The expense and inconvenience of techniques such as modem dial-back and passworded modems is unnecessary.

Threats from Authorized users

o **File browsing**
Many users, especially those not expert in computer system use, are minimally aware of the use of file protection mechanisms. As a result, files that may contain confidential information can be read by other users who are curious.

It was suggested that the default file protections for new users be changed from *world-* and *group-readable* to *user-readable*. There are two aspects to this question:

- desirability:
  (+) promotes protection and privacy
  (-) inhibits group sharing of information
  (-) requires a significant change in user habits

- feasibility:
  Implementation on both VMS and UNIX is trivial.

Recommendation: The committee felt it did not represent the user community sufficiently to recommend a change in default file protection.

This matter should be referred to the CSAC.

See APPENDIX I and APPENDIX II for further discussion.

o **Privileged users**
Although not known to be a problem, the possibility for abuse of privacy by persons with system privileges does exist. A clear statement of the responsibility for confidentiality on the part of persons with system privileges is deemed adequate.

o **Unauthorized machines**
Ethernet technology currently allows any host to masquerade as another. The number of hosts will rise dramatically with the availability of DECnet DOS and inexpensive

workstations such as the Sun. It is unlikely that anyone at LBL would attempt this method of breakin, but the problem could become significant when we connect the LBL Ethernet to the Campus Ethernet.

- **DECnet DOS**
  Persons using DECnet DOS should be made clearly aware of the potential for misuse. An unauthorized user who gains access to a PC being used for DECnet DOS access to the cluster could use information in that PC to break into the cluster account. DECnet DOS machines must then be housed in an area that has some level of security - i.e. an office, not a hallway or user area.

Computing Services Security Policy

(1) LOGIN ISSUANCE

A login request form, which includes name, lab address, employee number, and account number, *must* be filled out by each applicant. Applicants are required to display identification. The data on the application is checked with employee lists supplied by the personnel department.

Group logins are not permitted. Computing Services offers free training and consulting on how users may share file systems.

(Note: It is recognized that this policy is not easily enforced, as a user can share a login and password with a colleague and there is no further system detection or checking. However, the establishment of this policy has minimized a significant security problem caused when a group of students shares a login, and may give the login and password to their friends.)

(2) PASSWORD POLICY

Password cannot equal login name.

Changes of password cannot equal previous password.

Password must be at least 6 characters long.

Password cannot be all the same character.

Password cannot contain a recognizable part of the login name.

Password is not to be found in the Dictionary.

Passwords are not to be written into files or electronic mail.

Password must expire within 180 days of being issued.

(3) LOGIN EXPIRATION

Login is deactivated after 90 days of inactivity.

Login is archived after 30 days of being deactivated.

Initial login is deactivated after 10 days of non-use.

(Note: Logins expire only by non-use or inactivity. An unused login that is compromised could be used indefinitely unless it is detected by the Division Administrator.)

(4) VMS SYSTEM BREAKIN PREVENTION PARAMENTERS

Tight control is exerted over system privileges.

User is notified of login failures upon next successful login (i.e., wrong password used for that login.)

Five login failures (either invalid login name or wrong password) causes the login to become inactive for 1 hour and is termed a breakin attempt.

Sensitive files, such as SYSUAF, are alarmed to detect unauthorized access attempts.

The system manager is notified of breakin attempts on the following day.

(5) NETWORKS

We discourage network access using passwords and encourage the use of proxies.

Use of the default DECnet account by users is not allowed.

TYMNET access requires divisional accounts and passwords.

(6) CENTER PHYSICAL SECURITY

User access is restricted to the user terminal and I/O areas.

The doors to the user areas are unlocked whenever Computing Services staff is on-site. At all other hours, access to the user areas is via approved card-key

LBL security is notified whenever CS staff will not be on-site. Additionally, all doors are secured and the environmental protection systems are checked for automatic operation.

(7) SECURITY AWARENESS

Computing Services conducts an ongoing effort to keep the user community aware of the importance of computer security.

(8) REMOTE LOGINS AND ACCESS TO REMOTE HOSTS

.rhost entries should be aged and expired. (See Appendix III).

Computer Security Monitoring Group

ORGANIZATION

Computing Services has designated a person whose responsibility it is to provide active, regular checks for breakin attempts.

This effort is supervised by the LBL Computer Protection Program Manager. (The CPPM is a member of the Office of Computing Resources.)

This activity takes no more than a fraction of an FTE.

The duties of this person include:

(1) making random checks of network and login traffic for unusual login or search patterns or use of commands such as "who"

(2) making random checks of usér files.

(3) arranging for the installation of monitoring equipment to facilitate call trace-back when systematic breakin attempts are detected.

(4) Coordinating efforts of network vendors and law enforcement personnel when appropriate.

It is noted that communication regarding breakin attempts should NOT be done with electronic mail.

Stand-Alone Computer Systems

(1) Computer systems that are not networked to the rest of LBL are not included in our recommendations. However, the prudent manager will observe similar policies.

(2) We also point out that these systems are subject to DOE 1360.2.

Recommendations

This TPEG was formed shortly after Computing Services changed many of their security policies as a result of a series of network breakin attempts. We believe that their policies, properly enforced, are consistent with the level of security required by LBL computers.

However, we do see a potential problem with lax security practices on networked machines installed in research areas. The owners of these machines are often not concerned that they may either be a target of hackers, or become an intermediate hiding place for breakin attempts on other LBL machines. We recommend that policies similar to that now in place for Computing Services be enforced for all networked computers. We also recommend that the Computing Services person who checks for breakin attempts be empowered to extend that checking procedure to all networked machines at LBL.

Specifically, all networked machines must exercise the following control:

- control the issue of logins
- not allow group logins
- support password aging and expiration
- prevent default and obvious passwords
- prevent storing of logins and passwords in clear text
- allow monitoring of network access by Computing Services personnel
- register location of LBL Ethernet access with the Office of Computing Resources.
- register all ethernet interface addresses

Recommendation for CSAC

CSAC should discuss the implications of changing the default file protections from world-readable to user-readable, and make a recommendation.

Additional Recommendations;

- The CPPM should draft a policy regarding the confidentiality of information encountered during security monitoring. This policy should be approved by the LBL legal staff.
- A working group should be established to define and administer a lab-wide scheme for user IDs to simplify the problem of integrating shared file systems.

APPENDIX I

UNIX USER FILE ACCESS PERMISSIONS

Permissions for read, write, and execute are set by the UNIX system when directories and files are created. The default is all permissions on for the user, group members, and "others", i.e. the rest of the world.

When using the C-shell the system default can be inhibited by setting umask in the .cshrc or .login file; the value that umask is set to indicates which permissions are not wanted. For example, "umask 002" tells the system that the "others" are not to have write permission; "umask 022" tells the system that neither group members nor "others" are to have write permission; and so forth.

Currently, the system has no way to enforce restrictions on the permissions of files created. The system could be changed to turn off permissions that we don't think users should have turned on. Initially, it appeared that this could easily be done in the kernel; however, it is not easy because a general scheme would cause a lot of system software to fail, namely those programs that need all permissions turned on. Another approach is to try to maintain a umask value for each user, that we could initially set; the problem with this is that quite a bit of code would be required for the system to maintain a table of user IDs and umask values on disk, maintain an up-to-date copy of the table right in the kernel, and then get the uid and umask information from the table for each file creation and open. A complication is that there exists system software that we would have to modify to deal with situations involving files created with inappropriate permissions based on the user ID and umask data in the table.

Currently, a user has no way to tell the system which permissions are wanted, only which ones aren't wanted. A program would have to be provided that would allow the users to change the value in the above described tables.

We can provide a default .login that sets umask as desired.

Dave Cleveland

APPENDIX II

VMS SYSTEM DEFAULT FILE PROTECTIONS

The current default is SYSTEM:RWED, OWNER:RWED, GROUP:RE, WORLD:RE. The default can be changed. A philosophic argument can be mounted against having no WORLD READ/EXECUTE permissions. The security TPEG is not the forum for such a debate. It probably more appropriate to CSAC. Note that the GROUP permissions are of little importance here at LBL because Groups are not used.

A user in VMS creates file protections in a 3 tiered level:

1) new files have the protections associated with the current directory, if a protection mask exists; (someone must have created the protection mask)

2) new files have the protections given them by the user in a user specified SET PROTECTION DEFAULT command (that is the protection mask often issued in a LOGIN.COM);

3) new files receive the default SYSTEM file protection mask

Users who are not issuing a new SET/PROTECTION/DEFAULT command are most often using the default system protection mask.

Another area concerned users wanting to share files. Files can be shared in common logins, but this practice is discouraged because of problems associated with file ownership. Examples of problems:

- o the directory can only be owned by one user and when a second user creates a new file in that space, the second user now owns files in the first user's directory;
- o there now arises an issue of quota; in fact if the second user has no quota on the disk, they cannot create a file or edit a file
- o the automatic movement of files for disk management becomes much more difficult automatic procedures resolve ownership problems by assigning file ownership to the parent directory.

VMS provides the tools to share files more accurately through the use of ACL (Access Control Lists). Users who are sharing files will also likely want to take advantage of CMS (the VMS Code Management System). CMS is a method for the straight-forward tracking of changes made to files.

The suggested pattern for users needing common files is that each user will get a separate login. Within that login, they will run DISKLOGICALS and then SET DEFAULT to the common area and then run a common LOGIN.COM so that they all create a common environment. Computing Services will have created and assigned to each user an IDENTIFIER. This IDENTIFIER will be used in conjunction with the ACL that is associated with the common file space. Any new files created or edited within the IDENTIFIER will have that same IDENTIFIER. Any user granted that IDENTIFIER will be able to do normal file manipulation. An ACE (Access Control Entry) will indicate which IDENTIFIERs have permission to WRITE or READ those files. There are provisions to install additional items on the ACE like CONTROL and SECURITY.

While this discussion may be confusing and not easily followed, Computing Services can install the required IDENTIFIER's and ACL's. Once installed the use of the IDENTIFIER's and ACL's is transparent to the users. The creation and editing of files is no different than before IDENTIFIER's and ACL's were installed.

Eric Beals

APPENDIX III

UNAUTHORIZED FILES (*ftp* OR EQUIVALENT TO GENERIC ACCOUNTS)

1) Any user who has logins on any two UNIX systems can equivalence the two logins and thus log in to one system from the other without having to provide a password. The same is true of transferring files – no password is required. Note that the logins can be different; all that is required is that the user make an entry with the remote system and login name in a *.rhosts* file in the home directory on each system.

   There are problems with respect to simply eliminating the remote permission files, *.rhosts*:

   a. during a remote login ("rlogin") the system does prompt for a password if no *.rhosts* file exists, but in the case of remote command executions ("rsh") and remote file copies ("rcp") the system is not able to prompt for a password;

   b. some of the system software is dependent on being able to execute "rcp" and "rsh" from non-interactive processes, i.e., processes that would not respond to a password prompt.

2) Use **procsl** file access mode under VMS.

This report was done with support from the Department of Energy. Any conclusions or opinions expressed in this report represent solely those of the author(s) and not necessarily those of The Regents of the University of California, the Lawrence Berkeley Laboratory or the Department of Energy.

Reference to a company or product name does not imply approval or recommendation of the product by the University of California or the U.S. Department of Energy to the exclusion of others that may be suitable.

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