LOGICAL DATA CORPORATION

Software Product Description

Brochure 10.2 06/04/99

Features

- **System Manager controls: security requirements, security file, system level password, security reporting**
- **Security passwords can be required for specific ports and/or user names**
- **Previous use message indicates date, time, and port to help detect security intrusions**
- **Users without access to sensitive information need not enter passwords**
- **Passwords of users are not available to the System Manager or other information system personnel**
- **Password status based on time elapsed since password creation or change**
- **Password users are prompted to change passwords periodically**
- **Purging of expired passwords is automatic**
- **Password reinstatement is controlled**
- **Automatic disconnect after too many illegal passwords entered**
- **System Manager controls: length of elapse periods, number of retries allowed, welcome message text**
- **Security violations logged if used in conjunction with TSX Logging Support**

TSX User Security System

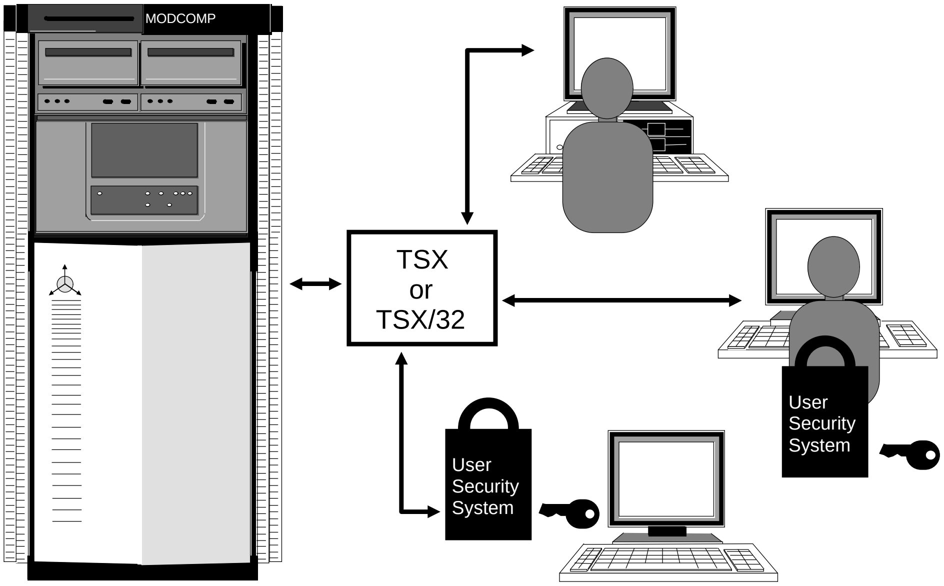


Figure 1: Enhanced Security for TSX Systems

The TSX User Security System allows the security built into TSX to be expanded with a flexible, site controlled, time managed password system. It is designed for use on MODCOMP CLASSIC+ or Tri-Dimensional+ computers running under the MAX IV or MAX 32 Operating Systems.

TSX itself requires a valid user name at log on to control computer access within the limits set for the terminal in use and the user name specified. The user name can be kept secret from other users, but it is accessible by information system personnel. The TSX User Security System provides additional security by requiring a password as well as a user name for some or all terminals and/or for those users who have access to sensitive information and programs. A user's password is known only to the user, not to the Security System Manager or to information system personnel.

The Security System Manager establishes a security control password, known only to himself, that governs access to the security file. To ensure privacy, the location and structure of security information has been encrypted to make it extremely difficult to analyse or decode.

Functional Description

Password Management

To make the system even more secure, the life of any user password is transient based on time periods defined by the Security System Manager. Passwords may remain valid and unchanged only for a specific time period. During a second time period, the user will be required to enter a different password at his next logon (passwords may be changed by the user as often as desired). Whenever a password is changed, the user will be required to verify the change by reentering the new password. When the correct password is entered, a message is displayed indicating the date, time, and port when the password was last accessed as a confirmation to the user that no one else has used his password. If a password is not changed within the required time period, the password becomes inactive and cannot be used unless it is reinstated by an authorized operator. If the password is not reinstated, it will eventually expire and be purged from the security file. The program to purge expired passwords may be cataloged as a pre-scheduled task (activated by a timer), or it may be executed as a batch overlay.

The Security System Manager is the only person allowed to add records to the security file. Thus any owner of an expired password or any new user must be issued a temporary user password by the Security System Manager before password protected terminals or user names may be used. The user will be required to change the temporary password during its first use.

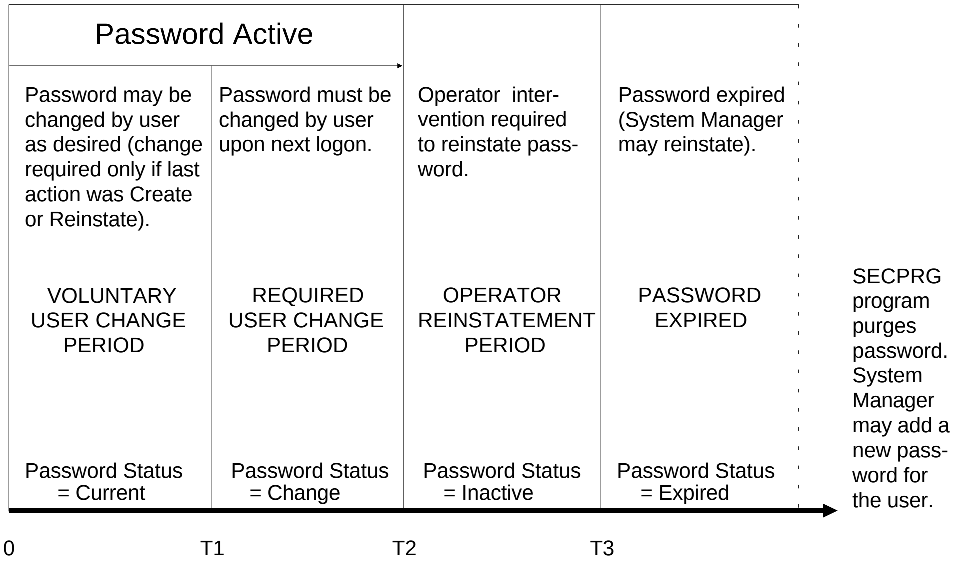
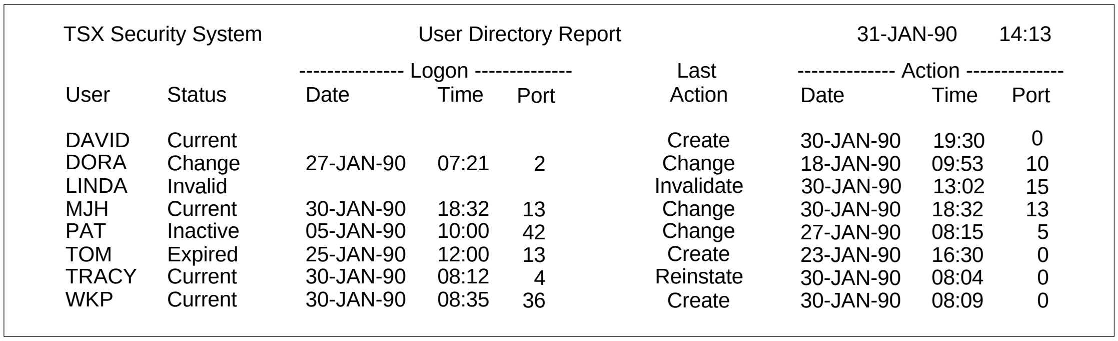

Password Active
Password may be changed by user as desired (change required only if last action was Create or Reinstate).
Password must be changed by user upon next logon.
Operator intervention required to reinstate password.
Password expired (System Manager may reinstate).
VOLUNTARY USER CHANGE PERIOD
REQUIRED USER CHANGE PERIOD
OPERATOR REINSTATEMENT PERIOD
PASSWORD EXPIRED
SECPRG program purges password. System Manager may add a new password for the user.
Password Status = Current
Password Status = Change
Password Status = Inactive
Password Status = Expired
0
T1
T2
T3

Figure 2: Security Password Age and Events



```
TSX Security System             User Directory Report                      31-JAN-90    14:13

                              --------------- Logon -------------      Last      -------------- Action --------------
User      Status        Date           Time     Port             Action       Date          Time      Port

DAVID     Current                                                Create       30-JAN-90     19:30      0
DORA      Change        27-JAN-90      07:21      2              Change       18-JAN-90     09:53     10
LINDA     Invalid                                                Invalidate   30-JAN-90     13:02     15
MJH       Current       30-JAN-90      18:32     13              Change       30-JAN-90     18:32     13
PAT       Inactive      05-JAN-90      10:00     42              Change       27-JAN-90     08:15      5
TOM       Expired       25-JAN-90      12:00     13              Create       23-JAN-90     16:30      0
TRACY     Current       30-JAN-90      08:12      4              Reinstate    30-JAN-90     08:04      0
WKP       Current       30-JAN-90      08:35     36              Create       30-JAN-90     08:09      0
```

Figure 3: System Manager's User Directory Report

Security Violation

The Security System Manager can specify the number of invalid passwords that may be entered repetatively before the security system terminates the user's session and instructs TSX to lock or disconnect the port to prevent further access.

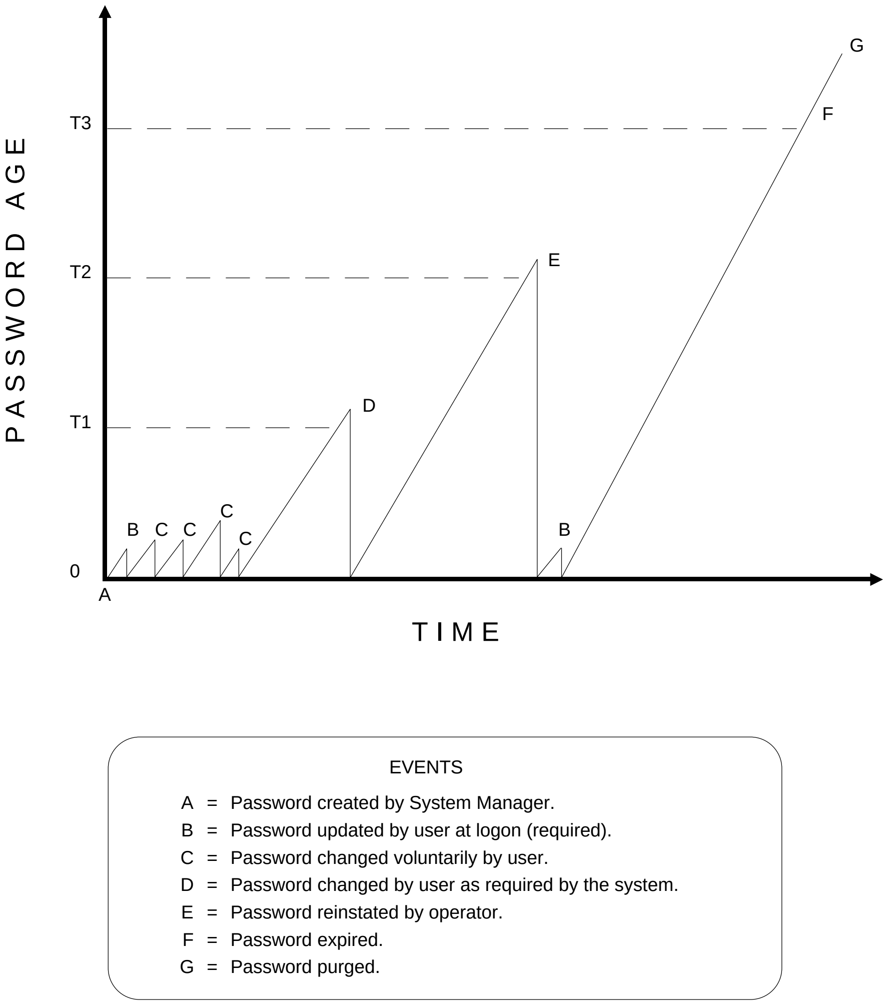
Logging

Security violations and purging of passwords will be logged if the TSX Logging Support is installed.

Security System Reports

The Security System Manager has sole access to the User Directory Report displayed by the TSX User Security System. This report shows each user's TSX alias name and the status of each user's password. See Figure 3. The Logon Date, Time, and Port indicate when and where the user last logged on to the system. These are blank if the user has never successfully logged on with the password currently on file. The Last Action and Action Date, Time, and Port columns display information about the last action taken by the system regarding the password of each user.

Each time one or more user passwords are purged from the security file, a User Purge Report will automatically be printed listing the purged records. The data printed for each record is the same as that shown in the User Directory Report in Figure 3.



EVENTS

A = Password created by System Manager.
B = Password updated by user at logon (required).
C = Password changed voluntarily by user.
D = Password changed by user as required by the system.
E = Password reinstated by operator.
F = Password expired.
G = Password purged.

Figure 4: Password Age and Events

User Interface

The TSX User Security System uses standard conversational mode I/O for all interactions to permit access by any type of terminal.

Installation

The software includes an installation procedure, which can be used without modification on most systems. Only minor changes are required to the existing SYSGEN and to the TSX Task Generation.

ADDENDUM

The following provisions have been established for Software Licensing, Installation, and Maintenence for the TSX User Security System.

Documentation

Each TSX User Security System license includes two reference manuals. Additional copies can be purchased.

Licensing

The TSX User Security System is a licensed software product and requires receipt of a completed, written LOGICAL DATA CORPORATION PROGRAM LICENSE AGREEMENT prior to shipment. This Agreement provides in part that the software and any part thereof may be used on only the single CPU on which the software is first licensed (provision is made for a backup system), and it may be copied in whole or in part (with the inclusion of the Logical Data Corporation copyright notice and proprietary notice(s) on the software) only for use on such CPU.

Code Availability

The TSX User Security System software is provided to customers in object code format.

Software Release Media

The standard release of the TSX User Security System is provided on either 9 track 800 or 1600 BPI magnetic tape. Software can be provided on alternate media subject to additional media and labor charges.

Installation

Software may be installed by the customer or by Logical Data Corporation. Telephone support is provided by Logical Data Corporation without additional charge to assist customers during installation. On-site installation assistance can be provided by Logical Data Corporation at additional charge. Specific information and fees regarding on-site installation may be obtained by consulting the LOGICAL DATA CORPORATION PRODUCT CATALOG or by contacting Logical Data Corporation.

Maintenance

Each TSX User Security System license includes one year of software maintenance, which consists of telephone support for on-site product problems, software corrections, and all enhancements. After the first year the customer may continue maintenance under the LOGICAL DATA CORPORATION SOFTWARE MAINTENANCE AGREEMENT.

Customer Services

Logical Data Corporation supplies a complete range of services including consulting, configuration design, site planning, installation, training, and support.

The technical contents of this document, while accurate as of the date of publication, are subject to change without notice.

+ MODCOMP, CLASSIC and Tri-Dimensional are registered trademarks of Modular Computer Systems, Inc. The trademark information is, to the best of our knowledge, accurate and complete.

LOGICAL DATA CORPORATION

P.O. Box 501528 Malabar, Florida 32950-1528 (321) 723-7000 FAX (321) 725-4086 http://www.logicaldata.com