

Thoughts concerning

How secure is your System ?

Joerg Groessler; Technical University Berlin

Presentation Abstract

Presentation Title: Thoughts concerning "How secure is your System ?"

Author(s): Jörg Grössler

Title(s): Dipl.-Ing.

Address: Technical University Berlin, Sekr. HE3,
Einsteinufer 19; 1000 Berlin 10

Abstract: (No more than 200 words)

Data security is an essential aspect of online computing systems.

It must ensure that internal data cannot be accessed by unauthorised
persons and that the file system can be rebuilt in case of a hard-
or software disaster.

In this paper components of the security system of MPE are presented
and analyzed. Weak points are highlighted and the measures necessary
to improve security are discussed.



What data security means

- o to be able to rebuild the file system
in case of a disaster
- o to restrict access on various type
of data

Standard File Backup Facilities in MPE

- o SYSDUMP, RELOAD
(based on magnetic tape)
- o STORE, RESTORE (tapes)
- o User Logging
(based on disc or tape)
- o Private volumes (disc)

Problems with Standard File Backup

- o tape read error during RELOAD
 - system cannot be started
 - next action "must be RELOAD"

measures:

- change disc packs before RELOAD
- RELOAD with 'ACCOUNTS-only' then
RESTORE the remaining files
(very time consuming)

- o tape read error during RESTORE

- all files stored behind error point
cannot be restored

measure:

- use RESTORE- or GETFILE2-program

- o user logging causes system overhead

measure:

- consider special logging during
program design

Prospects for tape-backup system

- o GETFILE-facility will be
improved
- o special STORE-RESTORE system is
considered (this possibly includes
features like UPDATE and APPEND)

Restrictions in Data Access

- o account-system (users, groups, accounts with different passwords)
- o user capabilities (SM, PM, PH, etc.)
- o filenames with passwords
- o privileged files
- o file access capabilities on user/group- and file-level
- o RELEASE/SECURE-commands

Possible seven Ways to crack the System

1. FIELD.SUPPORT

measure:

Password on SUPPORT-account
or remove SUPPORT-account
from the system

2. Jobs in PUB.SYS-group

measure:

password on job-file or
put job into other SYS-group

3. LISTUSER @.@;LP

measure:

log-on-UDC or perform command
not in PUB.SYS-group

4. Open all files of the system

measure:

special analysis of system logging

5. Read terminal buffers (PM-capability
needed)

measure:

remove PM-capability

6. Reading tapes

measure:

keep track of all tape-transactions
also using system logging

7. FOPEN on terminals

measure: ??

8. ...