

*Saltzer*

TO Hardcore Group Distribution  
FROM: D. R. Vinograd  
DATE: March 18, 1970  
SUBJECT: System Security and Failure Problems

The following is a list of known security or failure problems as of March 18, 1970. At the present time no manpower has been assigned to correct these bugs. Further additions to this list are solicited as are persons volunteering to fix these problems.

*user can change his own user id to anything he likes*

<u>Type</u>	<u>Problem Description</u>	<u>Remarks</u>
Failure	Access on process_dir_dir allows *.*.* rewa	User could delete any users process directory including initializer
Failure	Bug in 'status' primitive referencing a branch with more than 100 names	
Failure	Many parity errors on TTY channel can cause destruction of software maintained tables	'Listman Bug'
Security	Print Daemon can read and delete another users files to which user does not have access when he makes request.	New Ring 0 primitive needed to return effective user access.
Security	User can gain control of EPL/Print Daemons by placing in his working directory a module they reference and being the first requestor of daemons service	Dummy request or forced prelinking could solve this problem.

*EPL Daemon will rewrite object segment through a link in my directory to someone else's directory without need to have access to the other daemon*