PROTECTION ON "SPECIAL PRIVILEGES"

Chuck Wall

February 27, 1974

Technical Memo TM.74-8

In my travels (wonderings really) through the TENEX code (at least let us agree to call it code for the purpose of this memo), I find that it is useful to jot down ideas on protection as they occur.

I am currently looking at the .LOGIN JSYS and it occurs to me that there are ways to control the operator, wheel,...etc., special user capabilities.

1) We could do away with all special user capabilities. (This may prove to be unworkable.)
2) We could limit them to a single fixed terminal. (This may prove to be un-political.)
3) We could signal the operator (the real operator, not just some guy with operator capabilities) that someone is attempting to login with special capabilities, whereby the operator could have the final say. For instance, the operator can stop the login entirely or provide the user with exactly the subset of the capabilities he needs to perform the function desired. The operator could also establish time limits in this category.

This, of course, presumes we have a trustworthy operator. In any case I throw out these ideas--if in your view they appear worthless--you can throw them out also. I certify that I have the capability to pass on the capability that will enable you to throw these ideas out in case you do not have the right to remove them from your environment.

The obvious point is that not only must we recommend protection policies and mechanisms to prevent illegal access to objects, but we should

also consider monitoring methods to detect such attempts and logging functions that will maintain an audit of all legal access to some set of highly sensitive objects.