A NOTE ON LIPNER'S COMMENT ON THE CONFINEMENT PROBLEM

by J. H. Saltzer

Lipner[1], in his comment on systematic ways of solving the confinement problem[2], accidentally illustrates the subtlety of the problem. He says "Either the *-property or the high water mark...can solve the confinement problem for storage channels." Earlier, he summarizes Weissman's[3] work: "...the 'high water mark' rule sets the classification of any new object that a subject creates to that of the highest classified object the subject has read.

The high water mark rule, in the course of sealing off channels of information flow, can introduce a new channel of its own. If a process can create new objects, and the existence of those objects can be detected regardless of the relative classification of the object and the prospective detector, then object creation itself can be used as a communication channel. For example, to communicate a 10-bit message, the putatively confined program need merely create some number of objects (fewer than $2^{10}$); that number can be detected by any less classified job in the system. Some additional rule is needed to prevent this possibility.

The so-called "*-property" appears to prohibit detectable object creation[4], and therefore avoids this built-in problem. Since solution of the confinement problem for storage channels occurs whenever the *-property is in force, and not under any other condition yet demonstrated, I suggest renaming the "*-property" the "confinement property".


This note is an informal working paper of the Project MAC Computer Systems Research Division. It should not be reproduced without the author's permission, and it should not be referenced in other publications.