Copies: Clark Wilhelm Schroeder Gridley

UNIVERSITY OF SOUTHERN CALIFORNIA

INFORMATION SCIENCES INSTITUTE

4676 Admiralty Way/ Marina del Rey/ California 90291

(213) 822-1511

30 August 1973

Dr. Jerry Saltzer
Massachusetts Institute of Technology
545 Technology Square
Cambridge, Massachusetts 02139

Dear Jerry:

The enclosed paper documents the security flaw in Multics Bulk Card Input. The technique I reported to you for utilizing the flaw to penetrate the system (by creating a link to an executable object program) will not work since the deamon marks the deck read-only. We have come up with several other techniques which are described in the enclosed paper.

Sincerely yours,

Richard

Richard L. Bisbey

RLB:blr

Enc.

28 August 1973

USC/INFORMATION SCIENCES INSTITUTE

Multics Bulk Card Input Security Error

An operational procedure is provided in Multics to allow users to input decks of cards. A deck to be so inputted must be immediately followed by an end of deck card as specified in the MPM and must be preceeded by a header card containing the following four fields:

1. Deck format - indicates the format of the deck so that Multics can perform code conversion.
2. Directory - is the path name of a directory into which a link to the segment containing the information in the deck will be placed.
3. Link name - the name to be given to the link placed in the directory.
4. Principal identifier - the name of the principal who is to have access to the segment containing the information.

Some time after such a deck is submitted to Multics operations an operator will input the deck by issuing the operator command read-cards from a SysDaemon process and placing the deck in the card reader. The read-cards command reads the deck, without the header and end cards, into a uniquely named segment in the directory >daemon_dir_dir>cards performing any necessary code conversion. It then gives read access to the specified principal (the principal identifier could specify all users, i.e., be *.*.*), and places a link with the specified name in the specified directory. This link points to the segment in >daemon_dir_dir>cards. Messages giving the name of the link and the success or failure of the above operations are output to the operator. The deck is then held for pickup by the submitter. It is the responsibility of the submitter to make a copy of the segment before it is deleted from >daemon_dir_dir>cards at some later specified time.

The Problem

The problem arises because the specified link is appended to the specified directory by a SysDaemon process. Since SysDaemon processes have access to almost all directories in the system, this gives a submitter the ability to place a link to a segment containing data of his choosing in virtually any directory in the system. This is almost like being able to create segments anywhere in the system. If a penetrator places such a link in a directory early in the search path of a process, he can substitute his own segment for the segments of other users in computations of other

users without the other user's knowledge. Because only read access is granted to the segment, only read-only segments may be substituted. Innumerable different types of penetrations are possible using this technique; the following are a few of the simpler more obvious ones:

1. The penetrator places a link named "start_up.ec" in the home directory of a user not already having a start-up segment. This will cause the data in the segment to be treated as Multics commands and executed immediately upon theuser next logging in. This allows the penetrator to take over control of that user's process without the user's knowledge.
2. Place the link with the name of some system data base not residing in the system library >sss in the directory >sss. Since >sss comes before other system libraries in the search rules, the penetrator's segment will be found before the system segment, thereby effectively replacing the system data base.
3. Multics System Tapes, i.e., tapes from which the supervisor segments are read, are generated on-line on Multics. Copies of all supervisor segments are kept in a specific directory in Multics, >library_dir_dir>hard> object. New systems are generated by placing all the newly modified supervisor segments in another directory off >library_dir_dir>hard with the name of the new system and picking up versions first from the new directory before looking for the old copy. If a penetrator places a link with the name of a supervisor segment not in the new system, in the new system directory it will be placed on the new MST and will appear in the new system when it is installed.

One of the important aspects of this penetration technique is that it is not traceable to an individual because the submitter of a deck is not identified.

The Solution

It is not practical to stop this penetration technique by having operators check submitted decks, because they would have to examine every card. The only reasonable solution is not to create links at all, but instead, to notify the user that his deck has been read in and where it is by some other means such as mail.