Copy to Saltzer ✓ Daley

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

Reply to: Project MAC
545 Technology Square
Cambridge, Mass. 02139

Telephone: (617) 864-6900 x6201

6 October 1970

To: Project MAC Group Leaders

From: R. C. Goldstein

Subject: Terminals, again

Like the weather, people have been talking about terminals for a long time, but maybe something is finally about to happen. I am attaching a memo from Bob Scott summarizing last week's Terminal Committee meeting. You will note that we are supposed to meet again very shortly to report progress on identifying requirements and desirable features. To date, I have had very little response from you. Our charter, by the way, covers displays and other kinds of terminals as well as typewriter-like devices.

I would like to elaborate a bit on a couple of issues regarding the Datel offer mentioned in my previous memo. You will recall that these machines would not offer either print inhibit or ribbon shift. We have become used to these features, but because of the potential cost savings, it is worth while to review their actual value.

The ability to selectively emphasize part of a message (i.e. through printing it in red) clearly has value. However, a couple of arguments can be made suggesting that it is not of critical importance. In the first place, display terminals which should be coming into much wider use, obviously do not offer red shift. Therefore, programs probably ought not to depend on it. It is true that there are alternative ways of emphasizing part of a display (italics, blinking, field reversal, etc.) but many display are not capable of any of these. Secondly, the red-black distinction disappears when the printout is Xeroxed or multilithed, which also reduces its usefulness. It should also be noted that, historically speaking, ribbon shift appears on M.I.T. terminals only because IBM requires this RPQ as a prerequisite to the one that does print inhibit.

(extra desk image instead)

Most people would agree that some mechanism must be provided for preserving the security of passwords. Up to now, we have always used the print inhibit function for this purpose. However, there are a number of feasible alternatives. Many commercial time

sharing services have the computer type a sequence of random characters in the field where the password will be typed; a reasonably effective, if inelegant solution. Many military installations make use of one-time-only passwords. The user provides the computer with a list of passwords. Each time he uses one, the computer removes it from the list. When they are all gone, he provides another list. This seems to me to be more trouble than it is worth.

As a reasonable alternative, I would like to propose the use of algorithmic passwords. This would work in the following way: Instead of typing "Password:" as is now done, the system types "Please respond" followed by a ten digit random number. The user then types something. The system passes the random number and the user's response to a procedure which returns a boolean indicating whether the login should be permitted. The procedure, of course, must be capable of being unique to each user as is now the case with conventional passwords. Ideally, in fact, it might reside in each user's directory with execute access given to the system and all other access denied. This would permit a user to "change his password" any time he wished.

Obviously, the response typed by the user would normally be some function of the given random number. The function should be easily computable in one's head, yet difficult to reconstruct by looking a a sequence of queries and responses. Numerous classes of functions fit this requirement. This memo is probably not an appropriate place to describe their properties in detail but I would be happy to discuss it with anyone who is interested. Furthermore, it is not even necessary for the response to be related to the input. A perfectly reasonable, if very simple, response might be the time of day to the nearest hour plus the day of the week.

I would very much like to have indications of feeling on the above issues. Also, we have some other good possibilities for replacing 2741's that involve purchase rather than lease. To help us evaluate this type of offer, what do you think is the estimated useful life of a Selectric typewriter computer terminal. We currently have about 50 at MAC. How many of these do you think will be around two years from now? three years from now?

Thanks very much for your help.

INFORMATION PROCESSING SERVICES
OFFICE OF THE DIRECTOR

CAMBRIDGE, MASSACHUSETTS 02139
ROOM 39-565 (617) 864-6900, Ex. 4104

October 1, 1970

Memorandum to: M. I. T. -Harvard Terminal Committee
Professor J. E. Bishop
Mr. J. E. Austin
Dr. N. Zachary
Dr. C. F. J. Overhage
Mr. W. J. Burner

The first meeting of the M. I. T. -Harvard Terminal Committee was held on September 29, 1970. Present were Messrs. Austin, Daugherity, Gragg and Spiro of Harvard and Messrs. Berlan, Burner, Goldstein, Scott and Van Vleck of M. I. T. At that meeting we agreed that the Committee should proceed along the following general plan:

1. Harvard and M. I. T. will each advertise the existence of this Committee as soon as possible within their own communities.
2. During the month of October the Committee members from Harvard and M. I. T., operating as two separate groups, will work at outlining hierarchies of present and potential terminal needs in their communities and at identifying ideal devices to meet these needs. At the Committee meeting scheduled for October 14th, we will review the progress being made in these investigations and will discuss how to summarize the information being compiled.
3. At the end of October, the results of these two surveys will be drawn into a working document to receive wide circulation at each Institution. This document will serve as a basis for comments and, after editing, will become a functional specification of need.
4. At the October 14th meeting, we will devote some further attention to identifying those parameters that we think should be optimized and to outlining the various trade-offs involved.

5. During the month of November, a final report will be prepared to describe the functional specifications and relevant trade-offs for terminals to meet the M.I.T.-Harvard need on a long-term basis. That report should also contain recommendations on how each Institution should proceed in the short term to avoid future incompatibilities.

6. After the report has been circulated, a seminar will be held at which the results will be presented and discussed and to which members of the two communities, other interested parties, and potential terminal manufacturers would be invited.

Our next meeting will be held on Wednesday, October 14th at 2 p.m. at the Harvard Law School, 518 Pound Building, 1563 Massachusetts Avenue, Cambridge, Massachusetts.

If you are unable to attend, please call Mrs. McSweeney on Extension 2092.

Robert H. Scott
Director

RHS/p