PROJECT MAC February 7, 1973

Computer Systems Research Division Request for Comments No. 4

REPORT ON TRIP TO CAMBRIDGE, ENGLAND

by M. D. Schroeder

Attached is the report of my trip to visit the memory protection research project at the Computer Laboratory of Cambridge University, England.

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.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

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

Telephone: (617) 253-6039

February 2, 1973

To: Mr. Marvin Denicoff
Program Director
Information Systems
Department of the Navy
Office of Naval Research
Arlington, Virginia 22217

Re: ONR:430:MD:klh
NR 049-189
27 December 1973

From: Michael D. Schroeder

Subject: Trip Report: Cambridge, England, January 14-20, 1973

Late in 1969 Professor M. V. Wilkes and Dr. R. M. Needham at the Computer Laboratory at Cambridge set up a new research project in the area of memory protection and data security in multiple access computer systems. Their aim is to develop an experimental multiple access computer system that supports user computations involving several (possibly a large number) independent, user-defined domains of access privilege. The project is funded by the Science Research Council. This work parallels work in the same area by the Computer Systems Research Division of Project MAC carried out over the past seven years. The purpose of my visit was to allow an exchange of ideas in this area of mutual interest.

The visit can be divided roughly into two phases. The first two days I spent getting acquainted with the members of the Computer Laboratory and reporting to them on our work in protection. This culminated in a seminar given by me on the material from my recently published Ph.D. thesis, "Cooperation of Mutually Suspicious Subsystems in a Computer Utility".*
In addition to faculty, staff, and research students from the Computer Laboratory, the audience included D. M. England and J. M. Cotton from Plessey Company, Ltd., and M. M. Smith from the English General Electric Company (GEC, Ltd.), all of whom made a special trip to Cambridge to hear the seminar.

* Project MAC Technical Report TR-104.

Almost all of the audience had thought quite deeply about protection problems. As a result it was possible to dispense with the usual introductory remarks on the value of protection mechanisms in computer systems and on the identity of the hard problems in the area, and launch directly into a detailed discussion of the mechanisms described in the thesis for passing arguments on calls between independent domains of access privilege in a computation. The seminar was quite well received, and one feature of the mechanisms I described led to the discovery of a flaw in their mechanisms for passing arguments on cross-domain calls.

After the seminar I had a brief opportunity to discuss the new and very interesting Plessey System 250 with England and Cotton. This is a general purpose, multi-processor, multi-memory module system designed specifically for real time applications such as telephone switching and radar control. They provided me with copies of 9 papers describing this system, which has made use of protection capabilities to achieve the high reliability required for such real time applications. A bibliography of these papers is attached to this trip report.

The second phase of the visit covered the last three days. I spent this time in discussions with Wilkes, Needham, and several research students learning the details of their new protection system, generally referred to as the Cambridge Capability System.* As a specific vehicle for their research into protection systems, they are building a computer system which embodies their ideas. This machine, which includes a micro-programmable processor being constructed at the lab, is expected to be running by October, 1973. They emphasize that this computer is <u>not</u> the prototype for anything, but just a means for deciding how much hardware support for protection systems would be economical in the commercial world and a means for exploring the implication of their protection mechanisms on all system aspects. They hope some of the ideas manifest in this computer will influence the design of commercial machines, but are not trying to produce a commercially viable machine.

* The only paper currently available on this project is:
Needham, R.M., "Protection Systems and Protection Implementations," 1972 FJCC, pp. 571-578.

The approach they have taken in organizing the capabilities that represent the different domains of access privilege in a computation is quite different from the approach we have explored at CSR. Rather than treating segments as indivisible, atomic units of information and managing capabilities implicitly on behalf of the user, as we do, they allow segments to be nested and allow (require) explicit user-produced code to manipulate capabilities to reference them. A single capability segment contains the union of all capabilities for referencing segments of all domains associated with a process. The selection and restriction of these capabilities that represents a specific domain in the process is defined by use of indirection tables. It is possible to constrain the selection of segments available in a particular domain in arbitrary ways by suitable construction of the indirect tables. Segments are addressed by specifying an indirection table and offset within the table. An offset within the segment is also provided. The meaning of an address depends on the indirection tables available at the time the address is used. As a result, each domain of a process has its own address space, and it is necessary to translate all addresses passed as arguments on cross-domain calls. On the other hand, addresses of fixed elements of a particular protected subsystem can be invarient with respect to the process in which it is executing, so such addresses can be compiled into pure procedures. One nice feature of this organization is that the use of many domains in a process is practical, possibly as many as one per procedure.

A second area in which the Cambridge Capability System is attempting to advance the state-of-the-art is that of process scheduling and control. Their basic idea is that any process ought to be able to spawn subprocesses for which it becomes the scheduler and coordinator. The result is a hierarchy of processes. The environment at each level is intended to be general enough that the operating system could be run inside of itself as a subprocess. As part of implementing this idea, a clever hardware interrupt handling scheme has been devised that automatically stores the machine state in whatever location is designated as the register dump for the executing subprocess by the immediately superior coordinator. This generalized process structure has profound implications on the structure of the system, and Wilkes, Needham, and company are now in the process of tracing these implications. This work should lead to insight into the relationship of inter-process communication and protection.

In one respect the research project at Cambridge is already a success. It has generated an almost endless supply of graduate student research projects in exploring the implications of the protection and process structure on every aspect of the system, e.g., file system, fault handling, memory management, I/O, interprocess communication, and multiple processor allocation. In general I was quite impressed with the quality of the work being done. I feel certain it will increase our understanding of the way to organize computer systems to protect information. It is my opinion, however, that the specific mechanisms they are considering go well beyond current or foreseeable practical protection needs. Their work, however, may lead to cleaner implementations of simpler, more constrained mechanisms adequate to meet currently perceivable protection needs. The trip was quite valuable in establishing close technical communication between the research efforts at CSR and at the Computer Laboratory.

31 January 1973

M. D. Schroeder

BIBLIOGRAPHY OF PAPERS ON PLESSEY SYSTEM 250

The Plessey System 250 is a multi-processor, multi-storage module, general purpose computer system that is specifically adapted to the processing and reliability requirements of real-time application such as telephone switching, message switching, and radar control. Reliability is achieved in part from a capability oriented addressing structure which prevents errors in one part of the hardware/software system from affecting the correct operation of other parts. There now are available enough papers on this system to develop a fairly good understanding of its design objectives and the implementation techniques used to achieve them. These papers are listed below.

1. Cosserat, D.C., "A Capability Oriented Multi-Processor System for Real-Time Applications," International Conference on Computer Communication, Washington, D.C., October, 1972.

2. Cotton, J.M., "The Operational Requirements for Future Communications Control Processors," International Switching Symposium, M.I.T. June, 1972.

3. Crompton, J.M., "Structure and Internal Communications of a Telephone Control System," International Conference on Computer Communication, Washington, D.C., October, 1972.

4. England, D.M., "Operating System of System 250," International Switching Symposium, M.I.T., June, 1972.

5. England, D.M., "Architectural Features of System 250," Infotech State of the Art Report on Operating Systems, 1972.

6. Halton, D., "Hardware of the System 250 for Communication Control," International Switching Symposium, M.I.T., June, 1972.

7. Hamer-Hodges, K.J., "Fault Resistance and Recovery within System 250," International Conference on Computer Communication, Washington, D.C. October, 1972.

8. Hemmings, W.A.C., "Telephone Switching based on System 250," International Switching Symposium, M.I.T., June, 1972.

9. Repton, D.J., "Reliability Assurance for System 250. A Reliable, Real-Time Control System," International Conference on Computer Communication, Washington, D.C., October, 1972.