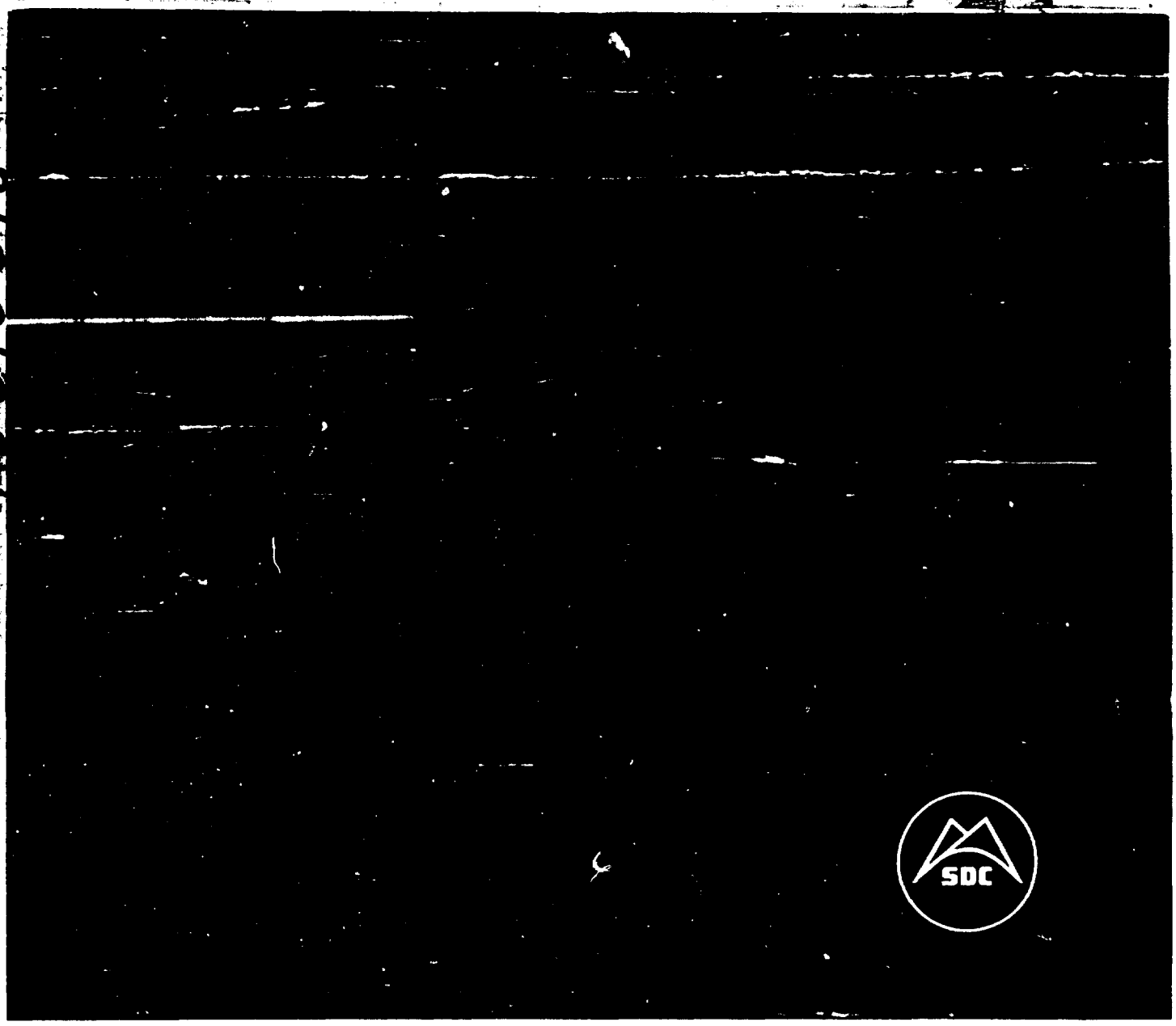

SP-2440/000/01

SECURITY IN THE COMPUTER ENVIRONMENT

Robert L. Dennis

18 August 1966

SP 2440/000/01

SP *a professional paper*

SECURITY IN THE COMPUTER ENVIRONMENT

Robert L. Dennis

SYSTEM DEVELOPMENT CORPORATION
2500 COLORADO AVE.
SANTA MONICA
CALIFORNIA
90406

August 18, 1966

A Summary of the Quarterly Seminar, Research Security Administrators - June 17, 1965 Santa Monica, California

INTRODUCTION

On June 17, 1965, System Development Corporation hosted a conference in behalf of the Research Security Administrators to look further at the problems of safeguarding classified information in relation to computers and computer technology. The meeting was the second of what is hoped will be a series of conferences to explore the many aspects of this general subject, ranging from the security aspect of time sharing to the protection of computer storage media.

This summary is a digest of the presentations made by the panelists and includes some floor discussion on various topics as they were given. Research Security Administrators would welcome comments on this paper as well as suggestions of ways and means to best continue and broaden the extent and scope of these studies.

WELCOME ADDRESS

Dr. Donald L. Drukey, Manager, Research and Technology Division,
System Development Corporation

A computer being operated in a time-shared mode raises a number of problems in security and need-to-know control. We also have the added problem of compartmentalizing the information for use. We need guidance from the security community that will tell us what it is that we of the technical community have to do to convince you that you ought to perhaps grant a clearance to a computer. We would like to know, for example, how much evidence do you have to amass, how many checks do you have to make, what kind of system do you want, and will it be sufficient to have a system that will tell you if somebody is tampering with it, or do you have to know they cannot succeed in picking the locks. These are the kinds of questions we need answers to. The only solution for some big installations has been to clear everybody who has access to the machine to the maximum classification level of any of the information being processed, and yet even here we forget about or ignore the need-to-know requirement. As we go to bigger and bigger systems, this problem will become intolerable. What we need now are guidelines as to what kinds of evidence we ought to be acquiring so that we may go about getting these clearances by putting some of the locks and combinations in the right places.

INTRODUCTORY ADDRESSES

Will A. Cummins, Head, 7094 Computing & Programming Branch, Data Processing Department, System Development Corporation

Insuring the security of information in a computer in a time-shared environment, insuring the security of information stored on and erased from magnetic storage, and insuring the security of electronic radiation eminating from a computer processing classified information are all problems that require attention. The main objective of this meeting is to describe our problems and to make you aware of our need for extended guidance.

Ellis P. Myer, Head, Liaison & Coordinator, Programming Systems Staff, Technology Directorate, System Development Corporation

Time sharing is many people using one computer system simultaneously. We have on our system at SDC up to 53 users; however, the average load at one time is 15 to 20. We have to store these various programs since there are more used than a machine can handle with one auxiliary memory. The IBM Q-32 with its magnetic core storage required a second computer to handle teletype messages, and the two different computers required a buffer so they could talk to each other. This handled the storage problem, but as it is now anyone who knows how to use our system may call and use the computer along with those of us who will be using it right here in-house. The system now has 15 or 20 users with individual programs and their own individual data stored for use with the computer. We are now trying to make sure that one person does not have access to another person's data.

TIME-SHARING SYSTEM DESCRIPTION

Robert F. VonBuelow, Head, Laboratory Development & Operations Staff,
Technology Directorate, System Development Corporation

In a time-shared computer system, a number of users are operating simultaneously, each with his own completely independent program. (A program is a series of commands, instructions, etc., that are stored in the computer that he is using.) If, either accidentally or on purpose, one user is able to get access to another user's data, there would be a breach of security if the second user were operating in a classified mode. There are many places throughout the time-sharing system where the data from one program are mixed with the data from another program. The user always knows where these data are, but the problem is how do we keep other people from getting it.

The obvious solution to the problem is to prevent access to a program by anyone but the authorized user. To be able to do this, one must positively identify the user and block out any unauthorized users. An assumption one must make is that the computer operators who are operating on the console must always be authorized personnel. Almost any control can be overridden from the maintenance console.

Positive identification of classified data breaks down into two classes: If the classified users are within the same general area as the computer, that is, if they are in the same building and the switching facilities of the telephone company are not used within a classified area, then the identification could be such that anyone who had access to a particular device likewise has access to the programs which can be associated with the particular channel to which the device is attached. The computer can easily distinguish one channel from another.

If the classified users are at some remote terminal, it becomes a different problem. Line tapping is possible and identification would then have to be by some other means. If the lines are considered secure but the device is not,

perhaps one could have some type of password arrangement. If the lines are not secure, which would usually be the case, then the problem is different--but not the problem I am addressing now.

The problem that now remains is how to block these unauthorized users from gaining access to classified data. The solution to this can be implemented in a number of different ways--by hardware-things built into the computer, by programs, or by some combination of both. Probably all manufacturers of large computers, and most of the manufacturers of small computers, have built into their machines a device or a part of a system called memory protection. Memory protection in a system such as ours is necessary for more reasons than security. One of the main things the programmers sitting at the consoles do is debugging of programs.

All programs, particularly new programs, are fraught with all kinds of errors. If an error on one program causes it to jump into the part of storage holding another program, and it <u>is</u> able to do that, this second program will likewise be disrupted. If this jump goes into the area that is holding the executive program, i.e., the program controlling the scheduling of programs, then everyone is in trouble. Some kind of memory protection is necessary for just these kinds of reasons. Let's consider any kind of a computer memory as a long list of words. A programmer is assigned some particular block within this long list in which he can work. There are a number of ways to keep him within that block. For example, each of these words has a unique address. Every time the program performs some instruction we can compare it with the boundary addresses within which the program must reside, and if it stays within this area, fine and good. If it tries to get out of this area, the computer does something to say, "No, you can't do that."

In the time-sharing mode of operation there is an executive program which schedules who runs and when, how long they run, and what area of storage they go into. When an error or perhaps a willful jump is made outside of the area

to which a programmer is assigned, this executive program takes control and stops that particular program, or informs it that it has made this error and prevents it from getting into the protected area.

The question is, how good are these protection schemes? Can they be violated intentionally or accidentally? I think the way to handle this particular problem is to have an unbiased expert try. For every new computer and every new computer system, a new trial and a new expert who knows the system intimately, who knows all the tricks a programmer might use, and who knows the hardware of that particular system, will be needed. This is not an accountant or a bookkeeper; this is somebody who is a programmer and probably an engineer as well.

At present, when we discover some of these tricks of how to violate a memory protection scheme, we keep them a secret. We keep them from everyone so that some other system which is not so protected cannot be violated. This has to change. There has to be some kind of an agency which gathers together and disseminates to the people concerned all the ways a system can be violated. For example, when we got our Q-32 computer, it didn't have a memory protection, it wasn't operating in a time-sharing mode, and the kind of mode it was operating in didn't require that we worry about this particular problem. We built in the memory protection ourselves and it was quite adequate. But when it came to operation, we found there were various ways this memory protection could be skirted. We put one of our experts on the problem and said, "Sit down and figure out all the ways you think you might be able to violate memory protection," and he did this. He figured out more than a dozen different ways. For some of these we were able to add hardware to positively prevent further violation. To others we made software corrections, changes within the program to keep people from these particular violations. As far as we know, now nobody violates the memory protection. Nobody can get out of an area to which they are assigned in our particular computer.

Probably most of the protection schemes we have found, or that other people will find, can be used by this central agency as a core of techniques to disseminate to various people. We feel a large number of these things are going to be common to all computer systems and if we have some agency that can take care of this, I think we have made a step in the right direction.

The points I would like to see come out of this particular meeting are: (1) Conduction of studies of possible methods of breaking security protection and solutions for any new breaks that are uncovered. Perhaps a variety of agencies should conduct studies such as this; (2) Collection and dissemination of data on means of protecting programs within the computer by some central clearing agency; (3) Designation of an expert by some authoritative body to verify or deny the security of each system; (4) And then, of course, selling to whomever the governing agency is the fact that this computer is secure, and that it can operate with classified or non-classified programs with no worry of compromise.

QUESTION: Are these breaches in some areas just theoretical or actually accomplished by outside agencies?

ANSWER: The work that we have done was not with a content of classified data. It was with two programs we wanted to isolate just to keep them from clobbering one another. This has indeed happened and had happened many times before we had any form of memory protection. I would venture to say that since we have put in both hardware and software protection techniques, we have had none. At least none that I know of. It might have happened to some programmer but since it didn't particularly bother him, we didn't hear about it.

One other point I would like to make is that in our new computer complex we are getting a large duplex computer to take care of all the jobs of the whole Corporation, including the one that you saw

on the Q-32; two computers tied together to do the job of research and development plus the production jobs and some secure jobs, such as programming for SAGE. There are other types of sensitive programs, payrolls for instance. In ordering this computer, we specified that one computer must be separable from the other by manually operated switches. Then when we go into a particular mode where we are worried about security or sensitive data, we flip the switches and the machines are physically isolated. This is quite a limitation on the system. It means that each processor doesn't have available all the storage or all the terminal devices; it has only half of them. Likewise, all the terminal devices or the users at these terminals do not have access to the whole memory. This is hindering the system quite a bit, and to have to go this way is a real crime. As the systems get bigger and you are tying computer to computer, it's going to be unbearable.

QUESTION: What type of instructions have you had from ARPA relative to the security aspect?

ANSWER: The instructions we have had are that when you are operating in a classified mode, you disconnect all the people outside of the building. Pull their plugs--pull all the teletypewriters out so they cannot get in. Dr. Drukey: That's not strictly true. ARPA didn't give us guidance. We said that prudence at this stage of the game says you shall do it that way, and that's what we have done.

QUESTION: Yes, but that doesn't solve the problem of the unclassified research.

ANSWER: Dr. Drukey: What we have done is when we have operated with classified materials in the programs, we have kicked everybody out who should not have access to that data. But we have restricted our customers at that time to those people who could reasonably be said to have clearance and need-to-know to that data.

QUESTION: Do you have classified data stored?

ANSWER: Yes. What we have done about that is to take the tapes off. We have established procedures which have been accepted for erasing the drums, erasing the core memory, and erasing the discs.

QUESTION: I would like to go back to the statement of a few moments ago. I interpreted you didn't like scramblers.

ANSWER: No, that isn't true. I said that isn't the particular problem that I was addressing. Scramblers are fine.

QUESTION: If you have to operate the way you just mentioned, you are losing the efficiency of the entire system, where with a scrambler you could continue to operate, could you not?

ANSWER: If they would be accepted.

Dr. Drukey: If we had crypto equipment, then presumably wherever we had a crypto link, we could keep that link connected. At this stage of the game, we feel we have to physically disconnect every non-controlled entry point, even though it appears to be idle, in order to go into a classified mode. You should be able to operate with an intermix of secure and non-secure access, however.

Robert Von Buelow: Even if we did have these crypto links, we would still have the problem of utilizing approved memory protection techniques.

QUESTION: Is it possible to permanently erase classified material from a disc and a tape?

ANSWER: I will leave that question to one of the next two speakers.

SECURITY OF ERASING MAGNETIC STORAGE MEDIA

Willis Ware, Head, Computer Sciences Department, The RAND Corporation

For a computer to operate successfully it has to be designed so that any information written into a storage device overwrites, or if you like, erases, whatever was there previously. We write into stores and we read from them. The act of writing, for the moment at least, is considered to include erasure of previous information.

Let me summarize one side of the security problem that Mr. Von Buelow has already touched upon; that is, unauthorized reading from any of the magnetic storage devices while they are connected to the machine. This is the big problem with time-shared systems.

A programmer can, either accidentally or deliberately, gain access to another man's information, be it in core memory or on tape, drum or disc. All four storage mediums are subject to the same problem. As Mr. Von Buelow pointed out, the safeguards against unauthorized access are partially hardware and partially software. In my view at least, neither alone is sufficient. In the extreme case, one would probably encrypt the information and put it into the machine, and this would protect it whether it was on disc, drum or tape. Can classified information which has been written on one of these magnetic storage devices be destroyed in the security sense without physically destroying the device itself? In this connection security people usually think of declassification as total destruction. Paper is burned, film is melted, and devices are destroyed. No effort is made to destroy the information per se. At present you are trying to deal with computer information in the accustomed way; destruction of the device or of the information-carrying medium. In this case, the incentive not to destroy the information carrying device is an economic one. We prefer not to melt down the tape, or to hack up the disc, or to junk the drum. We need to look into the problem of destroying the information without destroying the device which contains it. The computer is designed to read

from its storage devices only the most recently written information. It cannot penetrate recorded past history in the storage devices; its designers do everything they can to make sure it cannot. From the point of view of devices permanently connected to the machine, the problem of declassification is solved by erasure, provided we can, in fact, erase magnetic surfaces completely.

Since the computer reads only the most recent information, it would appear to be sufficient to only require writing nonsense information over the classified information. If one can assure himself, "one" probably being you security people, that writing does in fact occur and that it does in fact occur over all regions of the magnetic storage device which contains classified information, then declassification has taken place.

There are such procedures specified today. One example is in Air Force Regulation 205-1, which specifies that streams of random digits written over classified information at least three times is sufficient to declassify. The reason for multiple writing is simply to make certain that all the classified areas have been covered. There are certain kinds of software failures and certain kinds of hardware failures in a computer which could negate the intent of this overwriting of nonsense information. So to avoid such failures, the regulation requires repeated writing, and it presently specifies at least three times. This procedure will certainly work for magnetic drums. The issue that is open for the moment, and which we will have to return to, is: will it work for tapes?

The tape problem is complicated by the fact that tapes are removable. A reel of magnetic tape can be taken from the machine and subjected to electronic or magnetic tampering. A disc pack can also be taken from its transport and presumably, therefore, is also susceptible to similar tampering. Reels of tape are taken from the machine just as you take a reel of tape from your hi-fi tape transport. Disc packs are taken from the machine exactly as you take a stack of records off your turntable.

As far as the machine is concerned, overwriting procedures can guarantee that past history is not accessible to the computer, and hence we can speak literally of the destruction of classified information. A roll of magnetic tape or a stack of magnetic discs is certainly susceptible to unauthorized possession. As such, they are subject to specialized laboratory techniques which might be able to recover the past history that the computer cannot. Just to speculate, one might treat the tape or discs with special chemicals; one might heat it and cool it, or refrigerate it, or what not. One might treat it with special magnetic fields or other special laboratory techniques and, in fact, recover information which has long since been overwritten and is not available to the computer. I understand that experiments have been performed which demonstrate that it is possible to recover information which has been overwritten by other information. The Air Force Regulation acknowledges the possibility of recovery of latent information, and it specifies that tapes once classified must remain so. Presumably they will also make a similar statement in an updated edition of the regulation about removable magnetic discs.

It is clear that experimental work needs to be done to discover how serious this problem is and to find out how it can be dealt with. We need to know if there are genuine erasure methods which will make the tape unreadable by any technique.

There is one more problem related to the previous one; what happens when you turn a machine back to its manufacturer or transfer it to an installation with a different security status? In general, a machine will have core storage--perhaps a drum, perhaps a disc, perhaps tapes. Each of these we will comment upon separately.

Overwriting into the magnetic core several times with streams of nonsense information will, as far as I can perceive, effectively destroy any classified information which may have been there. I know of no mechanism or laboratory techniques which would provide for the recovery of a latent image. I think

the magnetic core can be sanitized without difficulty. However, there is a long chance that one could take the magnetic core into the laboratory and extract things which are long since gone. Therefore, if one wants to be very careful, I think my statement should be verified experimentally.

Do the drum and the disc have the same problems as the tape? The economic considerations are a little more important here because of the high unit cost of magnetic discs and magnetic drums. I do not know right now if we are allowed to return a drum or disc to a manufacturer if it has once contained classified information. It may be that at this point in time, physical destruction is the only way out. Offhand, I would expect, speaking as an engineer, that whatever erasure techniques are demonstrated to be satisfactory for tapes will also prove satisfactory for drums and discs.

There is very little guidance available to us in industry as to how to destroy classified information contained in magnetic storage devices used as parts of the computer without destroying the storage medium. The incentive to solve the problem is economic. The Industrial Security Manual covers no aspect of the problem, and while one military regulation deals with part of the problem, it leaves much of it untouched.

I feel this is mainly a technical problem of really not much difficulty. I think I would feel able, given a dozen engineers perhaps and a handful of programmers, to deal with the technical aspects of the problem in a year or so. I do not think it is a serious technical problem. I think it is an important and maybe an overwhelming political and administrative problem, and so far as I can see, the real problem is to establish some focal agency to conduct tests, to establish standards, to determine policy, and to have the authority to promulgate and enforce its findings on the military and the industrial users who are charged with handling classified information in their computing centers.

QUESTION: Mr. Ware, and you were speaking in your own opinion I believe, when you said you felt that magnetic storage mediums are technically erased through rerecording or overwriting methods. In other words, that is a way of saving the total dollar loss on a roll of secret tape for a certain project. So, if you ran it through with random information or nonsense information or any other terminology you wish to use, then started it through the machine again with a new program of classified material, this would perhaps satisfy the requirement to protect the former information--is that right?

ANSWER: You are right. I intended to leave that impression. Let me clarify my answer a little bit. I should have restricted that comment specifically to magnetic cores, permanently mounted discs and drums. The problem with a reel of tape is that when you take the reel off, after you have presumably overwritten it, you would like to be able to think of it as declassified. However, the next time it's mounted on a tape unit the programmer will not write on it in exactly the same place you wrote on it or erased it, and so there is an outside chance that the old information will leak through. As long as the probabilities of leakage are not zero, then security people are not going to be satisfied and we have to go to heroic efforts to achieve certain erasure.

QUESTION: But here again, the worst that could happen when it is used again is that the person being involved with it would not have adequate need-to-know, but would still be allowed access because of his level of clearance?

ANSWER: Yes. This is the only reason I can think of for ever maintaining a magnetic tape as classified, aside from the possibility of it being stolen and given special treatment.

ELECTROMAGNETIC RADIATION FROM COMPUTERS

Jerome A. Russell, Computation Division, University of California,
Lawrence Radiation Laboratory

I am here to talk about electromagnetic radiation, and this we all have. Every machine radiates electromagnetic energy because of the wires transmitting current, and magnetic and electrostatic fields are generated by these--they are all actually little transmitters. The entire machine sends out radiation. Every time a magnetic tape transport starts and stops, you get wide bands of transmitted noise.

Our problem is to minimize the possibility of someone outside the fence picking up these noises, and they can be picked up if you have a sophisticated enough receiver.

At Livermore we have a radiation problem like everyone else, and you can't say, "Well, let somebody try to figure out what it all means," because that is not enough proof it's secure. I would hate to have this task myself; it would be a life-long job, I am sure. We do take pains to control the radiation as much as we can. The Edison Company lines coming in are all run through banks which have shielding in them. We do this to protect the computers, not necessarily to make the information secure, but it does keep the information from going back to the power lines.

With the teletype setup, we have a multi-programming or multi-processing system which we call Octopus. We have twisted pair cables carrying the teletype leads to the physicists' and mathematicians' offices. These cables are enshielded according to a classified regulation which says you have to have a shield on it of a certain nature, and we do. We don't share the telephone facility with regular voice-lined systems.

A physicist sits down at the teletype and, with his Calcomp plotter, he questions about 80 million dollars worth of computers on the other end. He says, "I would

like very much to look at pressure as a function of time." He types in that he wants to see a certain pressure on a certain scale factor. The Calcomp plotter then starts drawing. He looks at it and says, "Here is a large piece I want to see in detail." Then he asks to see the value at the peak and he gets a number back. This is typical of the communication that goes on between the physicist designing a weapon and the computer. Since nothing is identified in detail, we feel the information is fairly secure.

We are more worried about the fact that people can, at remote locations, generate documents which might possibly be classified without having the usual stamp or registration on them. We don't print what the graph is; we don't make the Calcomp plotter title it; we don't allow anyone to put units on the graph; so you don't really know whether it is millibars in pressure or volts. Perhaps there should be some investigation or tightening up of just what is generated.

Conventionally, the scientist would go to the machine room, pick up two or three feet of printout, go back to his office, and then reach the one number he is interested in. With the Octopus system, he can ask for that number without studying all the printout. We believe this offers a great security advantage in our multi-processing system.

One area where we need guidance very much is in photographic digital information handling. The nature of the mass-stored document is the unit record--a piece of photographic film which has little data fields on it in digital form. Each record holds 32 of these little chips of film in a plastic box, and these plastic boxes reside in large plastic trays. There are a number of these plastic trays which are moved back and forth mechanically and pneumatically. There is no regulation for holding documents of this kind. If the specifications for magnetic tape are sparse, specifications for photographic digital information storage are non-existent.

We see some distinct advantages in a system of this kind from a security

standpoint. For one thing, all of the information resides in one location--one room which can easily be guarded. Access to this equipment is allowed only to those people who are intimately concerned with the equipment. We don't have the problem of people taking tape out of or putting tape into a tape vault or leaving tapes on their desks in the office. They never take the documents out; they never see the documents. The amount of film going in, new film which has been unexposed, is easy to keep track of. In fact you must keep track of it so you don't run out. The amount that you destroy at the end is also very easily accounted for. You take out a box that has 32 chips in it and you burn the chips. Again there is no problem of using the medium over again or changing classification because it is not reusable; you must burn it to get rid of it. We have a manually administered library in conjunction with, by use of the same equipment, the mass storage and fast retrieval system. So again you have no more security problem than you do with magnetic tape. In fact you have much less because there is no particular advantage in taking the boxes up to your office; you can't get them out of the holders in the first place.

The Octopus system has one serious problem. Once in a while it fails, and when it fails it is very difficult to know what happened. Everyone's problem is either ruined or they all have to start over again. We have built in an automatic logging device which keeps track of every transaction that goes into the Octopus. If typewriter 42 goes in and asks for a particular thing, a particular area from the mass storer or magnetic tape, there is a mark made on a little strip of paper. We use this for restart information, so if the system goes down we can begin things all over again or do some diagnostics on what happened--who was last in it when it failed.

If someone asks for something to which he is not entitled to have access because of adequate need-to-know, we have a complete record of when he asks for it, where his typewriter is, and the nature of his request. We have built into our system an inability for a person to get into other people's files. There are general files like routines, common data which would affect a whole group of people,

and then there are specific areas. We haven't built these walls into the information for security reasons, although it turns out there is some advantage in them. We have done it so that somebody doesn't wipe out his friend's data accidentally. But the fact that the system will deny you access to things for which you have no business, that is, some typewriters and some log-in numbers will not gain permission but will log the fact that you tried, has particular advantages too. Again there is no security regulation regarding this. You can't read in the blue manual anything about what you should do with a log like this, or even that they recognize such a log for such a transaction. And yet it is not unlike a document library in which you have a librarian checking classified data in and out. It just happens that the volume is much greater. I am sure if you walked into the library here and asked the girl for all of the Top Secret documents, she would most probably make a note of it and call the Security Officer. This logging device does the same thing.

QUESTION: How do you identify that I am not authorized to get this information? That is assuming that I know the special word to ask.

ANSWER: If you know the special words to ask and you are sitting at one of several correct typewriters, then you will get the information. However, if an employee goes on vacation, the fact that he is not going to be asking for that certain number is cranked into the system so you cannot get to the information during his vacation. Each individual problem has a code. We haven't changed them yet, although one can imagine the scheme for changing them. Right now they are associated with the individual and the problem. If you state the problem you are working on, you are immediately prevented from getting into other areas of the computer. We are not trying to do any encrypting, although it is possible that the machine could assign different people something like the code for today is so and so. There are potentialities, but we are not doing that. Of course, if you remember, all the people there are "Q" cleared; they all recognize the problems of violating levels of need-to-know.

QUESTION: How about overwriting? Let's say it's getting signals from outside the place?

ANSWER: Where would they come in? There are no wires from the outside. The only way would be if you called somebody on the telephone and asked them to do this, but then again you would be violating the discussion of classified material regulation.

PANEL DISCUSSION AND QUESTIONS

MODERATOR

Will A. Cummins
Head, 7094 Computing & Programming Branch
Data Processing Department
System Development Corporation

PANEL MEMBERS

J. W. Lathrop
Head, Dayton Project
Technical Information System Department
System Development Corporation

Jerome A. Russell
Computation Division
University of California
Lawrence Radiation Laboratory

Robert F. VonBuelow
Head, Laboratory Development & Operations Staff
Technology Directorate
System Development Corporation

Paul Walsh
President, Matrix Corporation
Washington, D.C.

Willis Ware
Head, Computer Sciences Department
The RAND Corporation

Fred Weber
Corporate EMC Manager
IBM, Kingston, New York

GUEST

Gilbert H. Davis
Deputy Chief
Office of Industrial Security
Defense Supply Agency

PANEL DISCUSSION AND QUESTIONS

Will Cummins: In listening to the discussions that have gone on, one of the things that has become apparent to me is that there has been no indication of the problem of identifying what is classified and what is not classified in the computer. Let me quote a couple of examples from some of the Form 254's (Security Requirements Check List) which we have filled out for one of our contracts. In one of these it was indicated that output listings, that data which is used as the basis for generating the output listings, are in themselves unclassified, though the data which is printed out would be classified if there were a requirement for a special interpretative program to operate on that data. In the same Form 254, there is an indication that the data base which was built from cards is Secret when read in. If one listed these cards, they would in fact be Secret, but the data base contained in the computer is not Secret. What in fact is Secret information? How do we really go about identifying it? The changing of the format in some people's minds causes it to be non-Secret.

Paul Walsh: There are tapes which perhaps would be classified because they can indeed be taken into a laboratory; there are others that are useless by themselves.

Willis Ware: I couldn't agree with you more, but that's not the present security point of view.

Paul Walsh: But aren't we here to help modify the security point of view so that we may operate more efficiently and economically?

Willis Ware: That's a very practical attitude, but I don't think we can, at this meeting, make any changes in the basic tenets of security. The essence of security is that you derive a set of rules which will work for every case that comes along.

Jerry Russell: There is another problem also. Say you have a bill of material for some device and this bill of material includes a great many nylon bolts. This in itself is not particularly interesting except that the knowledge that this particular group is using nylon bolts in a particular device might tell them something about a triggering mechanism and of the inability to use metal around it. Any time we say that a reel of tape just has numbers on it or just a piece of some bit of information, we are saying that we can second guess all of the possible combinations of things which could be derived from this. I don't think this is too farfetched really. Little tiny clues often would unlock a lot of other things.

COMMENT FROM THE FLOOR: I would like to respond to what Dr. Ware seems to be saying. It's attractive to assume that one particular profession has a monopoly on logic, but I don't think, really, that either the engineers or the security people enjoy such a monopoly. I think that the economics of any system that you try to devise and the administration of that system need to be taken into consideration. We are trying to reach a solution to a problem that we both have inputs to, and it's not that either one enjoys a monopoly of talent for solving the particular problem.

Willis Ware: That's a well-taken point, but what's going to have to be done for us is first to update the Security Manual, and update it in such a way that each one of you, as you interpret it in his own fashion, is on safe ground. The practical issues, such as you have raised, are issues of interpretation not issues of the composition of the original regulations.

COMMENT FROM THE FLOOR: I think it goes back to the issue mentioned a few minutes ago and that is, everyone seems to make the assumption that given a reel of magnetic tape unidentified in any manner, someone dealing with it knows the basis of the information or the analogue information. You have to have a lot of other knowledge about a particular reel of tape before you can ever make any sensible deductions from it. So first we have to identify what is classified and how classified information is identifiable.

Willis Ware: For the purposes of this argument, a reel of magnetic tape is no different than a deck of cards. Security people have rules and regulations for handling decks of cards, and it doesn't matter what those cards have on them; the rules and regulations are uniform. A reel of tape is no different in that context.

COMMENT FROM THE FLOOR: From a realistic standpoint that deck of program cards or that reel of tape, and I am talking about an erased reel of tape, you have is unclassified unless you have other knowledge connected with it before you begin to analyze what it contains, particularly when it is overwritten or erased, or a combination of both, on a random reel.

This is the problem we are concerned with, not a tape that currently has classified information on it. We accept the fact that a reel of tape or any other storage device with information currently recorded on it which is classified has to be protected. That's one fact. The other fact that is becoming a more overpowering problem all the time is: what do you do with the things that can no longer be used for classified material? And again I refer to one of our pressing problems. We are constantly receiving analogue tapes, telemetry tapes, input tapes which are reduced and put on digital form. When we are through with the analogue tape, it can no longer be used for telemetry information. It has to be clean because of the noise problem, not because of security. We store these things forever, and we don't have that much use for digital tape, so they become dead storage. You mention these are expensive tapes, so the problem gets worse and worse. Now these can be erased, overwritten or what have you, but my question is still: what can you learn from this after it has been passed through this process? It comes back to the problem of what can you deduce from a random reel unidentified with its original use.

Willis Ware: You must be prepared to guarantee that it's unidentified.

COMMENT FROM THE FLOOR: You have to be prepared to insure they only get one magnetic tape and they don't have anything else. How can you insure this? This would be part of the problem of protection. Part of this thing we might be looking for is a way to let loose of these storage devices for some use other than classified. This is the answer I know we are looking for. I think that the answer that has been given by security agencies though is: once you have classified a tape you can't use it for anything else.

Bob Von Buelow: First, if you say that you can completely erase it, that's fine; the problem goes away. If there is something there, then you have to treat it like Willis said, like a deck of cards or a printout.

Fred Weber: But in answer to the other question posed, it seems to me what we are doing is challenging the government's cryptographic capability, and I don't think we are in a position to do that. I think they know a lot more about this than the people in this room. I think the problem here is that we keep thinking we are going to process a tape that has been erased back on the equipment and try and find something to use in the existing equipment. They are talking about equipment you don't even know about, and you don't know the technology involved.

QUESTION: Most people don't realize, I am sure, once you erase a magnetic tape, you can play that tape back after erasures and you will get garble--most people do not realize that these are external noises picked up by the sensitive nature of the tape which are meaningless. But within the government, they still contend that this is a conversation of the previous recording. Do you have any comment on this?

Fred Weber: We are talking about a highly classified area, and all I can say is that I had the responsibility at IBM for selling top management on a program that they do have this capability and they can demonstrate it if they want. They are not very cooperative as far as demonstrating this thing is concerned. We do work very closely with them, and we have experts within our corporation who have reached a capability where they know what they are doing.

QUESTION: Are you working on any program of research on better degaussing?

Fred Weber: Not that I know of. Not within my particular area. There may be some of the development groups handling this problem, but it is not in the EMC effort. But I think I'm going to propose a plan, after listening to this seminar, for next year or the remainder of this year that it be part of my responsibility.

COMMENT FROM THE FLOOR: If this is the case where an agency has the capability of recapturing data for these tapes, then we must presume that other people with other ideologies must have the same capabilities, and it looks as if we are faced with coming down to the practical security procedures and techniques for living with these problems.

Fred Weber: There is a specification out which says that if you operate under this illusion you are going to lose a lot of business. If you think that the specs are so stringent that you are not going to comply, you are going to lose business. Furthermore, this particular specification is going to get more stringent as the availability of equipment becomes easier.

COMMENT FROM THE FLOOR: Again I want to state the premises on which I was making my statement before. I will confine it to the fact that this digital recording has been degaussed and rewritten some number of times since classified information was on it. You would have to assume that you could reconstruct that tape in its entirety to match the printout. You would then have to work and find out what you can reconstruct and whether it contains any classified information. This to me gets to be astronomical in its probability.

Willis Ware: It costs you something to do all of these successive rewritings and degaussings. Once that cost exceeds forty dollars, you might as well have thrown that tape away in the first place.

Fred Weber: As soon as we get back to talking about the time-sharing aspects of the computers that are less than a year away now, or maybe some of them are actually in operation, I think we move into an area with a whole new set of problems. I further feel that unless the security community does the necessary research and sets down some definitive rules so that we can know how to operate under these conditions, we are going to grind to a halt very shortly.

Dr. Drukey: Within our contractual effort now we have authorization to go ahead on the question of: how do you secure a compartmentalized computer? The money is available; we can do it if somebody will tell us what we have to produce as an answer in order to get some of these rulings out and in the manual. Our problem is that we have talent and we have money, but we don't know what to do with it. Will you please help us? We have done and are doing the things we know about. We are going through the exercise of picking locks, trying to build better lock picks, and then after we build better lock picks we try to build better locks that those lock picks won't work on. But we need some guidance as to how good is good.

Will Cummins: I would like to ask a question of Gil Davis. What is your response to the question that Don Drukey posed?

Gil Davis: The only answer I can give you is that if you start a discussion in this area, you get into such a highly classified area that I've got to keep my mouth shut. It's as simple as that. The other answer is, what are we willing to pay to protect the security of the United States, and are we going to do whatever is necessary?

Joe Lathrop: I am in charge of some contracts which have to do with the design and implementation of the kinds of systems that create a multitude of problems like those you heard today and many others. I am overawed by the magnitude and spectrum of the kinds of problems you describe and the number of different problem areas that have been unsolved, so to speak. As a manager of these

contracts and being involved in implementing systems, I am in a position of looking for that focal point you were talking about where decisions are made on new kinds of security problems. I don't think we are going to solve here any large percentage of the technical problems. I think we can identify that focal agency and move that bit of work forward so that we have some place to go with those problems, and that focal agency has got to have more than just security backgrounded people. It's got to have some combination of security, engineering, and data processing background capability, so that when we have a new problem of the kind that needs a ruling, we have a place to go. We have some places to go now, but the link between what I call the intelligence community and the non-intelligence community is a very poor one. Many people and many agencies have made rulings on the kinds of problems that your people are struggling with. As an example, you talked about degaussing devices. It's been brought to my attention by my people in the Dayton Office that one government agency is now accepting a degaussing device. I think you can speak about it in that general sense. We have guidance in that direction.

I am against a great big program of experimental work. There are several things which I feel are necessary and more economical to look for in solving these kinds of problems as well as identifying this focal agency. Even though this solution gets overused now, the most practical solution is to determine the highest classification and require everybody to have that classification. This doesn't control your need-to-know, however. For this problem I think you have to control the access to your remote inquiry devices. I am a user of the SDC time-sharing system; I have a data base I have to protect. It's an unclassified data processor; we are protecting it. I am sure ours is a way which is unacceptable to present security standards, but I have no place to go for a ruling. Nevertheless, there are some techniques by which you can design diagnostic and internal programs to protect this information so long as you control the access at the remote inquiry point. I perhaps have a solution for the time being, but I don't have a place to go to determine if this solution is acceptable.

Control of access is still an economical answer to a good part of the problem we have here. The number of minute problems which actually occur and appear to require experimental laboratory work would necessitate a program so large that it would be uneconomical. The technology is so fast-changing, as Gil Davis pointed out in between sessions, that you could never catch up, but if you had a body ready to rule and knew of decisions that had been made in the intelligence community or in the DoD environment, you might be able to use some of these techniques.

You could program internal diagnostic programs for detecting need-to-know that would be satisfactory to security. When you are working with a time-sharing system, you are always doing a lot of battering back and forth; the machine is talking to you and you are talking to it on an immediate basis, and you can require a diagnostic check on this person's need-to-know. There is the engineering constraint that points up protecting parts of computer memory, but we need a body to go with it to say, "Is this enough? Can we get a ruling?" This, plus any engineered equipment, has to be according to certain specifications that are laid down. We have a start on the specifications handled by NSA. We have Federal Statutes available, but they are not known to many people within the local security agencies.

I go to my customer; I ask him for a ruling on something; he can't give it to me. He may not be aware that the decision has been made, maybe at NSA, maybe at CIA, or at least an acceptable solution offered. So we need a better link. What we can do in this kind of a session is begin to push for that capability at some focal point for decisions. That capability has to include engineering, data processing, and maybe other technologies, plus people with security background.

Dr. Drukey: I would also like to suggest that in addition to a place where you can get a ruling, we need to provide a clearing house for information for those of us that are conducting studies. It seems to me that the things we

have learned and the approaches we have tried ought to be of interest to a community trying to protect these machines. There ought to be some place we can go and say first of all, this is what we have to offer, and secondly; has anyone else experimented in this area and what have they learned? What have they tried on their machines that maybe we haven't thought of trying? That kind of a clearinghouse would be a useful tool.

Gil Davis: There is, or is supposed to be, an established agency under the Assistant Secretary of Defense called Installations Logistics. When it is operating, that may be the place to get your ruling, your technical rulings. A security evaluation upon the request from that agency will be forthcoming.

You mention why there aren't rules in the Industrial Security Manual on the area of magnetic tapes. There has always been the practicality of creating an arbitrary decision of what to do and the cost factors involved in accomplishing this. If you jump too fast, industry would object because of the cost factors in resolving some of these problems. We have deliberately held off. I am sure there has been more work done in a lot of these areas. In the area of degaussing, there is one item of equipment that has been accepted by a single agency. We are studying this in DSA to see whether we would use it. This is also debatable because you get the disagreements between the technicians. We haven't the overall solution; therefore, there has been no ruling set forth in the Industrial Security Manual. In the area of magnetic tapes we have given you guidance, and it has been out for a long time; namely, once material is classified, it shall be safeguarded from that time forth.

Will Cummins: It's clear that one problem which continually came up was the need for studies to be conducted in such areas as breaking security protection in the time-shared system, and also the potential need for additional work in erasing magnetic tapes, discs or drums. It's also conceivable, however, as the discussion indicated, that there has been significant work done that really needs to be disseminated. The prime need, many of us have felt, that has come

out of this discussion has been a need for guidance to be reflected in some authorized source--if not the Industrial Security Manual, some place--and last, the need for an agency to look into attempts to satisfy some of our ongoing problems of security.

Unclassified

Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) System Development Corporation Santa Monica, California	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

Security in the Computer Environment

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)

Dennis, Robert L.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
18 August 1966	31	

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
AF 19(628)-5166 b. PROJECT NO.	SP-2440/000/01
c. d.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this document is unlimited

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY

13. ABSTRACT On June 17, 1965, System Development Corporation hosted a conference in behalf of the Research Security Administrators to look further at the problems of safeguarding classified information in relation to computers and computer technology. The meeting was the second of what is hoped will be a series of conferences to explore the many aspects of this general subject, ranging from the security aspect of time sharing to the protection of computer storage media. This summary is a digest of the presentations made by the panelists and includes some floor discussion on various topics as they were given.

Preceding Page Blank

DD FORM 1 JAN 64 1473

Unclassified

Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Security **Classified Information** **Computers** **Time - Sharing** **Computer Storage**						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization *(corporate author)* issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year, or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers *(either by the originator or by the sponsor)*, also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through _____."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through _____."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through _____."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring *(paying for)* the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as *(TS), (S), (C), or (U)*

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.