An Interview with

DANIEL J. EDWARDS

OH 427

Conducted by Jeffrey R. Yost

on

2 July 2013

Computer Security History Project

Roanoke, Virginia

Charles Babbage Institute
Center for the History of Information Technology
University of Minnesota, Minneapolis

Daniel J. Edwards Interview

2 July 2013

Oral History 427

Abstract

In this oral history, computer security pioneer Daniel Edwards discusses his long-term career as a computer security researcher at the National Security Agency (NSA). He discusses Trojan Horse attacks, a term he introduced in the computer security field to describe a particular type of computer security vulnerability of hidden malicious code within a seemingly harmless program. He provides perspective on the evolving relationship of communications security (COMSEC) and computer security (COMPUSEC) at the NSA. Edwards became part of the NSA's National Computer Security Center and was principally involved with the development of the NCSC's/DOD's Trusted Computer Security Evaluation Criteria (TCSEC) and elaborates on the processes and considerations in developing and refining this influential set of computer security standards.

This material is based upon work supported by the National Science Foundation under Grant No. 1116862, "Building an Infrastructure for Computer Security History."

Edwards: I'm not sure how much I have to add to this, since I've been out of the business for about 35 years.

Yost: People generally go into the interview feeling that way and then we find they in fact remember a great deal and it's immensely helpful to our research. I'm here today just outside of Roanoke, Virginia, with Dan Edwards conducting an oral history for CBI's NSF-funded project, "Building an Infrastructure for a Computer Security History." This is the morning of July 2, 2013. I'd like to begin with a few biographical questions. Can you tell me when and where you grew up? Where were you born?

Edwards: I was born in Bridgeport, Connecticut. I grew up in Pittsburg, Pennsylvania; Cincinnati, Ohio; Shaker Heights, Ohio. After that went to school at M.I.T. The oldest of seven children so we had to move frequently in order to find a bigger house. [Laughs.]

Yost: Who were your greatest influences early in life, pre-college?

Edwards: Albert Einstein. I was a scientist constantly interested in many scientific sorts of things. In the fourth grade, this was after the atomic bomb had just been dropped, as part of an art project I did a diagram of a nuclear chain reaction and the art teacher didn't quite understand it. They sent me to the principal. The principal said wow and made me take it around the whole school to show it to every class, the diagram that I had done in the fourth grade. I started playing or being interested in computers in the seventh grade. I built an adder, based on diagrams in *Popular Science* or one of the early scientific

magazines. I collected a bunch of relays and put together a binary adder, and was interested in computers ever since.

Yost: Did that factor into your decision to go to M.I.T.?

Edwards: I was thinking of being a nuclear physicist and physics and M.I.T. seemed to go together. My parents both graduated from Cornell and they took me there first, but I was able to get into M.I.T. But when I found out what a physicist really did, I switched to electrical engineering because that's where the computers were.

Yost: Do you recall if you took any computer programming related courses at M.I.T.?

Edwards: I took every computer course they had. Not that I needed the particular material in the course but being a member of the course gave me access to the computers at M.I.T. And after I graduated, I started working for the Artificial Intelligence Project led by John McCarthy and Marvin Minsky. Part of the early work that we were doing was on the LISP computer programming. One of my first tasks was to write the first LISP garbage collector. We had the LISP program running on IBM 704 computers at the time. A number of research workers were using LISP for different projects. James Slagle was doing the algebraic; he would run his programs for about 45 seconds on the IBM 704 and he would be out of free storage and the program would stop. So after we got the garbage collector running he'd run for about 45 seconds, the garbage collector would kick in and run for about 45 seconds, and he would continue his computation.

Yost: That must have been fascinating to work with McCarthy and Minsky.

Edwards: Yes, it was certainly a very stimulating environment, both the LISP programming language and the time-sharing systems early on the IBM 709, 7090, and then the Multics system.

Yost: So was it initially CTSS [Compatible Time-Sharing System] you were working with?

Edwards: That was CTSS, yes. I wrote my thesis on an IBM Selectric typewriter, which was one of the terminals on CTSS, and my wife typed the thesis.

Yost: Do you recall if there were any privacy or security concerns with using CTSS?

Edwards: I wasn't particularly aware of that, but when Corby — you know, Fernando Corbató — introduced the idea that people had to sign on with some sort of a password there was some amount of resistance to that because that seemed to put barriers on the way of the community of people were using the computer.

Yost: There was a community of sharing.

Edwards: Yes, an open sharing sort of thing, and the notion of having accounts locked down or having a password was something which did not gain universal acceptance, at least at the beginning.

Yost: And what year did you graduate from M.I.T.?

Edwards: I got my bachelor's degree in electrical engineering in 1959. I continued studying at M.I.T. while I was working there so I had a master's degree in 1965 and electrical engineer's degree in 1967. The EE degree is essentially a Ph.D. without the thesis.

Yost: Did you have any involvement with the Multics project as it was being planned?

Edwards: Yes, I was one of the programmers on the Multics project. I've forgotten — well it was probably device drivers at that point, the code that I was working on. We were doing a lot of work in assembly language at that time. FORTRAN had come on the scene but when we looked at the code that was generated by FORTRAN compared with the hand-crafted assembly language, we said we could do much better than FORTRAN so nearly all that was done in assembly language. We also had fun after hours: Space War was a 1961-62 project and I was part of that team. Steve Russell, you know, led the team with the initial concept, but recruited help, essentially. I put in the code for the gravitational star in the middle, and the outline compiler which made the whole ship turn and be more responsive so that the code was able to execute within, oh, 30 milliseconds

or so, which means we had a fairly continuous display on the point plotting display, which came with the PDP1.

Yost: And was that a project that was done after hours?

Edwards: That was strictly an after-hours project; that was not part of the day job. But we had access to computers, we could use them after hours, and we did a number of interesting projects. You know, T-Square, which I didn't work on — a total time-waster — was a project to draw circuit diagrams for the Tech Model Railroad Club. It was probably a precursor of some of the CAD programs that came along a little later. It was a fun time.

Yost: And were you involved in any discussions or efforts surrounding the design of security principles or elements of Multics?

Edwards: No, I wasn't really involved in any of those discussions, or at least not as much as I remember at this point.

Yost: Okay. So one of the main projects early on that you worked on was the AI, and LISP, and then Multics.

Edwards: Right. And then transitioned to be part of the Multics group.

Yost: Were there any other projects you worked on at M.I.T. before going to NSA?

Edwards: I was working with Ted Glaser for a while, he had a PDP-8 computer. I was writing code for that.

Yost: Had he developed an interest in computer security by that time?

Edwards: He was connected with NSA at the time but I think that the work that he was doing was not directly involved with computer security. Oliver Selfridge was also in and out from Lincoln Labs. He was also connected to M.I.T. Work was going on at that time at Bolt, Beranek and Newman, with the initial IMPs, you know, internet message — I don't know whether we called it internet at that time. I've forgotten — something message processor.

Yost: Interface Message Processor.

Edwards: Yes, something like that.

Yost: I worked closely with Dave Walden on a couple things—IEEE Annals editorial board and the IEEE CS History committee I'm now chairing. I don't know if you know Dave, but he was involved in the project to develop the IMPs.

Edwards: I did a little moonlight work with BBN at the time, and one of the things that we put together was a data dial. That was a patent that was issued in 1965 plus or minus, using a dial telephone to input to a computer. It sort of worked. I put together the circuit which connected the telephone interface to the computer, because I had sort of a side career working in the telephone business. One of the projects which we did in high school was put together a small PBX for our house so that telephones in one room could call to another room and we didn't have to pay Bell Telephone, essentially, for the various extensions we had. Another engineering sort of thing which I was involved with.

Yost: What year was it that you completed your master's degree?

Edwards: Right, I believe that was 1965 and my engineer's degree, I think, was completed in 1967.

Yost: Was there a particular professor that served as your main advisor?

Edwards: I really don't recall.

Yost: You mention Ted Glaser and off the recording you asked if I interviewed James Anderson. Both of those individuals are people we really wish we had had the opportunity to interview, wish this was an earlier project when they were still living so that we could interview them. I'll ask you about Anderson a bit later, but can you tell me what you remember about Ted Glaser?

Edwards: Okay. Ted was blind but that didn't slow him down at all. He was technically very sharp, but also a terribly compassionate person. I enjoyed working with him, essentially on the PDP-8 computer. I think we may have had an early PDP-12, which was a miniaturized version of the 8, as I recall. So it was through Ted Glaser and Oliver Selfridge that they suggested I get in contact with NSA. They sort of facilitated the process of transitioning from M.I.T. down to Fort Meade.

Yost: Can you tell me a bit about the thought process you went through in making that career change?

Edwards: One of the things which I did in high school and also early college was have an interest in cryptography. I was a member of the American Cryptogram Association. They published a newsletter with examples of many different kinds of cyphers. I did handwork, essentially. Occasionally I would write small pieces of computer programs to work on things like that. Part of my thinking was of the old NSA deeply involved in cryptography and that was one of my latent interests, so it sounded like an interesting place to go to work.

Yost: That was in 1967?

Edwards: That was in 1967 when we made the transition from the Boston-Cambridge-M.I.T. area down to Fort Meade.

Yost: Before making that transition, you mentioned BBN. Did you have any connection with MITRE?

Edwards: We visited MITRE every now and then. There was also the Systems Command out at Bedford Air Force Base. But other than visits, we didn't have a connection to either of those projects.

Yost: When you arrived at NSA, can you tell me a bit about the environment and your first impressions?

Edwards: I guess I was somewhat in awe of NSA, at the amount of computer power they had at that point which dwarfed everything that I had access to before.

Yost: Probably dwarfed anything that existed anywhere at that time.

Edwards: Yes. The computers, which they had in the basement, were vastly more than anything I had seen before. But I was pretty focused with the initial position in computer security research, which is part of the research arm of NSA.

Yost: At that time was there a separation between the long-standing communication security side and the research program that included computer security?

Edwards: Yes. That is, the R&D folks' fairly small effort in computer security, the C folks in computers, you know, handled all of this stuff in the basement. S was mainly involved with securing communications. I don't recall much coming from S, which influenced the R&D stuff.

Yost: So there was R&D, S, and C were the groups.

Edwards: Yes, there were the three groups. And in R&D there was a group which was focused on algorithms, feeding directly into the S side of the organization but the part that I worked for really didn't have much in the way of connection with the folks in the S organization.

Yost: And so in R&D, there was the algorithms group there, the computer security group. Were there others as well?

Edwards: I'm sure there were but I really didn't poke around much. I had things on my plate which were quite sufficient.

Yost: Roughly how large was the R&D group overall?

Edwards: The computer security R&D group was, I'm thinking, on the order of 10 or less.

Yost: And do you recall what colleagues you worked with? Was Steve Walker there at that time?

Edwards: Steve Walker was there, Ed Spiegelthal was part of the group, Doug Hogan was the leader of the group.

Yost: Had Hilda Faust joined yet?

Edwards: Not yet, to the best of my knowledge. But one of the first things we got involved in was the Ware Report. The background which — material discussions essentially, which went under Willis Ware's chairmanship.

Yost: So that was a committee that you served on?

Edwards: I served as part of the technical staff on that committee; I wasn't doing the high-level thinking. I was a technical person who brought some programming expertise to the table and started thinking about different ways computers could be used or abused.

Yost: And so in that capacity, did you attend all the meetings for the Ware committee?

Edwards: I attended many of the meetings but I certainly was not part of the high-level drafting at all. I was simply providing technical input.

Yost: Before that committee was formed, Ware and Bernard Peters of NSA presented a paper at the Spring Joint Computer Conference in 1967, which was one of the earliest articulations of the computer security problem and probably the fullest piece of research ever presented on multilevel security to that point. Was that a paper that you were aware of?

Wright: I am quite sure that I was aware of the paper but I haven't read it recently. I'm sure there are a number of details in there which are simply escaping my mind.

Yost: Can you tell me what you remember about both your work, with regard to supporting the Ware committee, as well as just deliberations of the Ware committee?

Edwards: Let's see, I guess I'm going beyond the committee. I don't remember a whole lot about the individual committee meetings, because that was getting started essentially about the time I was sort of getting my feet on the ground with a new job at NSA. Some of the things that we got involved with a little bit later were looking at some of the time-sharing systems and trying to see where some weaknesses were. There were a number of folks that were building systems based on the time-sharing principle, and were influenced by the Ware Report, but were not very sure that their particular machines were able to separate between, say, classified and unclassified information.

Yost: Were you aware of any study of the committee of Multics and what it attempted to do with security, and what could be learned from it?

Edwards: Not directly. I think Roger Schell was quite influential in picking up that things that were put into the Multics processor in order to segregate things, and it was Schell who later took those principles, essentially, and went to the chief architect at Intel and talked about what needs to go into the Intel processors in order to be able to fully virtualize a machine. And at that particular time, the 286 was in production, but Schell's influence essentially influenced the design of the 386 to the point where the architecture could be fully virtualized.

[INTERRUPTION]

Yost: So we were chatting about the Ware Committee. Are there any other things you recall about the workings of that committee?

Edwards: Not really.

Yost: And what were some of the things that you worked on for the committee, specifically, do you recall?

Edwards: I think it was probably mainly had to do with abuses that one could take in existing time-sharing systems, plus the notion of being able to encrypt information and have the flow across the network encrypted end-to-end. The notion of end-to-end security, I think, was a very important part of that. And then trying to figure out how you

do that. This was clearly in the very early days of the ARPANET. In 1967, I essentially had very little understanding of all that was going on there.

Yost: Were any of your colleagues in the computer security research group at NSA also involved with the work of the committee?

Edwards: I don't remember. I'd have to look at the committee, at the report.

Yost: I don't recall seeing Walker's name on it.

Edwards: I don't either.

Yost: But it's been a few months since I looked at that so I'm not positive. I believe Glaser was on it. You mentioned the name of the group leader and I didn't jot that down.

Edwards: Doug Hogan.

Yost: Can you talk about his background?

Edwards: Not really. That is, I only knew him as the leader of the group.

Yost: Can you tell me a bit about how the group operated and organized work? Was there a good deal of freedom of individual researchers to pursue things or were there tasks assigned, or a combination?

Edwards: It was sort of a combination, as best I recall. I certainly had enough fun things to work on, at least from my point of view. Really didn't pay a whole lot of attention to the tasks that other folks were involved in.

Yost: When the Ware Report came out in 1970 it became the fundamental document describing the multilevel security problem with time-sharing. And [it] fundamentally dealt with open environments. NSA was a closed environment. Were there fundamental differences in how computer security was viewed at NSA versus some of the considerations being discussed in the Ware Report with regard to open environments?

Edwards: I don't recall a substantial difference because even at NSA, not everybody has access to everything. The "need to know" idea was heavily part of the culture and people were only cleared for certain activities. When it got to the point where you had folks in, say, a watch kind of thing that had a look across many different individual projects, you started wrestling with the idea of how do you preserve as much as possible in the "need to know" way of thinking, instead of simply clearing everybody for everything. It also wrestled with the ideas of how do you authenticate the individual? Does the individual have the right at this particular point in time to look at this information, or make that sort

of change? How do you transition that from person to person as they're on watch versus off watch? All sorts of things that we wrestled with.

Yost: I mentioned before, the paper in 1967, that Ware and NSA's Bernard Peters collaborated. Was Bernard Peters part of that research group that you talked about?

Edwards: He may have been part of that. I guess I'm confusing two Peters.

Yost: Yes, there are definitely two Peters in the early years of computer security, there's Bruce Peters and Bernard Peters.

Edwards: But there's also Rick Peters, who was part of the computer cryptography side of the business and sort of a sister to the part of R&D that I was involved with.

Yost: Ok. If I remember correctly, I think Bruce Peters was at System Development Corporation, onsite colleague of Clark Weissman at SDC.

Edwards: I am simply not connecting with Bernie Peters, at this point. I think Rick Peters went on to become head of the S organization. He was a cryptographer.

Yost: So through the years of the Ware Committee, until it came out in 1970, was that your principal research task?

Edwards: Yes it was.

Yost: Do you recall any of the other research projects that were being done by the research group in 1967-73 period?

Edwards: I really didn't focus on the projects that other folks were working on. I was asked to consult on some of the more classified things that were going on in the basement. I guess one of the notions that we were involved with was the notion of penetration teams. We looked at several systems, both internal and external to NSA. I remember the security officer, at least one of the security officers, being quite upset when we handed him his password for one of the systems that was supposed to be secure. We were able to read a little bit of code and look at some buffers that were involved with the drums which stored a lot of the information, and from that we were able to dig out the login credentials.

Yost: So this was probably, some of if not the first Tiger Team efforts done?

Edwards: To the best of my knowledge. But the notion of one of the threats, the Trojan Horse, was one of the things which contributed to the overall pot of potential threats. But we certainly, at that time, didn't see the computer virus kind of actor. I think that was largely due to the fact that we were not doing that much with the different connectivity of computers. That was still being developed but at that time, we were pretty much focused

on the standalone systems, and the power of essentially a lot of different computers being connected together was something which would develop a bit later.

Yost: So in the 1967-70 period you were interacting with the Ware Committee. Were there other interactions between you, as well as others at NSA, with the emerging computer security research community outside of NSA? Were there any conferences, meetings, or workshops in those early years that you recall?

Edwards: I really don't recall conferences and workshops. As things developed, some of the folks left NSA for different places. Dennis Branstad, for instance, went over to NBS. We certainly had occasional chats with the folks over at ARPA as the ARPANET was developing. The whole notion of a security kernel was being developed in the early 1970s. Roger Schell had a lot to do with that.

Yost: Can you tell me more about the contact and interaction with the ARPANET research? And in the end, was there any specific advice that you or others gave to members of that project?

Edwards: Not that I'm aware of. I think we were still trying to understand the whole process and since we didn't have many machines to work on at that time in terms of being connected with the ARPANET, NSA was still quite insular with respect to having systems connected to outside the building there. But as time went on, the notion of end-to-end encryption kept resurfacing because a number of military commands from

different places around the world would be receiving data from many different sources and needed to get back. We wanted to be as sure as we could that this sort of man-in-the-middle, somebody tinkering with the interface message processors or something like that, could not deal with at least the data that was being sent back and forth. So the notion of end-to-end encryption kept resurfacing and trying to figure out how to turn that idea into reality was some of the research that was going on in the 1970s.

Yost: Was Jim Anderson consulting with NSA and the computer security research at NSA in the late 1960s? I know he was a member of the Ware Committee. Did you get to know Jim at that time?

Wright: Yes. He was in and out on a regular basis ever since we were part of the computer security business.

Yost: Did your time at M.I.T. overlap with Roger Schell as a doctoral student at all?

Edwards: I'm not sure.

Yost: Did you get to know him back then or only later?

Edwards: I probably recognized him but probably didn't have much interaction with him at that time. Clearly, when he got involved with the projects at NSA I had more interaction with Roger.

Yost: And you became a member of the Anderson Committee, is that correct?

Edwards: Yes, but I don't remember a whole lot of the details of that.

Yost: Do you recall if it was Anderson or Glaser or who asked you to join that committee? As I understand it, Ted Glaser was officially chair but in many ways, Anderson took leadership of the committee.

Edwards: That pretty well matches my recollection of it, but then, as a sort of technical staff, I was sort of actively avoiding trying to take a management role.

Yost: I'd like to go through some of the committee members and see if you recall anything about their contributions to the committee in their work. Ted Glaser?

Edwards: I guess my only recollection would be more leadership rather than specific technical input.

Yost: Melvin Conway?

Edwards: I recognize the name but I really can't comment.

Yost: Steve Lipner?

Edwards: Sorry.

Yost: Your NSA colleague, Hilda Faust?

Edwards: I think Hilda was mainly a manager rather than a technical contributor. As I recall, she came from the communication security side of the house and as the various research and development organizations were formed and reformed, I was part of Hilda's group. At that time, we were more heavily involved with the ARPA folks and taking the first steps in terms of putting together end-to-end security.

Yost: You mentioned Roger Schell. Was Roger the one who first came up with the idea of a kernel, to your recollection?

Edwards: I think that the notion of a kernel of an operating system grew out of CTSS and became part of Multics, as Roger got involved, the notion of a security kernel really took shape. And a lot of work went in to trying to find a mathematical basis for being able to give very high degrees of assurance that a particular piece of code was operating as intended and didn't have side effects that could be exploited.

Yost: And that played into the work that Roger's group with the Air Force later funded with David Bell and Bell LaPadula, as well as the parallel Case Western effort with Ted Glaser, and others.

Edwards: I don't recall that much about the Case Western — you know I used to live in Shaker Heights, Ohio, and had friends in the late 1950s who were part of the computer lab at Case Western. And I wrote my first computer program as a result of one of those friendships in late 1957, as I recall. But I don't recall that much about what Ted was doing at Case Western. The work with security kernel led to some contracts with Ford Aerospace, Mike Pliner. There are some other names back there but it takes me about a day to come up with [laughs].

Yost: Long time ago.

Edwards: Names that I haven't dredged up recently.

Yost: What about Clark Weissman?

Edwards: He was the leader of the SDC contract at that time; made a number of trips from Fort Meade out to Santa Monica to review that particular effort. But I would really have to look at some additional reports to remind me of some of the details of that particular effort.

Yost: And was that the Adept-50 effort or are you talking about later work in which he was involved?

Edwards: I think it was later work.

Yost: Was Adept-50 something that was studied by the committee and did you have a sense of what was and wasn't achieved with Adept-50?

Edwards: I am drawing quite a blank, essentially, with respect to details about Adept-50.

Yost: Roger Schell talked about the security kernel concept in tandem with a reference monitor. Do you recall if that reference monitor idea was something here the committee came up with? I think this was in the early 70s — might be 1972 or 1973 — that was something Peter Denning and, I believe, Scott Graham wrote an early, pioneering article that dealt with a reference monitor.

Edwards: I guess I would tend to associate that with Roger, but that was probably based only on the contacts which I had. Reference monitor was, again, part of the effort to write mathematical proofs essentially that a piece of code was performing as intended and had no unintended consequences…. We recognized that even with a reference monitor, there was still the notion of covert channels, such that information could leak out of the system based on observables. Even down to how fast messages were sent out or not sent out, or even watching the power line as a signaling medium, and recognize that the notion of covert channels like that was simply something that we'd have to put up with. And the best we could do was make some kind of an estimate of what kind of bandwidths we

were talking about, and saying below a certain threshold there's not much we could do about that.

Yost: You recognized the vulnerability, and as I understand it, coined the term Trojan Horse. Can you tell me about the context of that?

Edwards: At the time, we were looking at different computer systems that would produce, say, cryptographic keys, other sensitive things and the notion that the programs that were running on these machines could be updated, since they were running on general purpose processors rather than application specific processors. So that the general notion that a program which appeared to be doing something useful could, in the background, be doing something which was clearly unintended came to mind. That is, the useful cover, and then the thing going on underneath, and it was sort of that connection that brought to mind the idea of something which looks good on the outside but has challenges on the inside — Trojan Horse — was simply a connection which I made and that got discussed in various forums.

Yost: Do you recall some of the earliest forums where it was discussed? Was it the Anderson Committee or . . . ?

Edwards: I suspect it was part of the Anderson Committee that I was looking at that reference in, what? 1971, '72, at the Air Force panel. There was another paper — and again, I don't have a copy of the paper, which I think was later on in the 1970s. As I

recall, it was at Princeton and I think both Anderson's name and mine were on the paper, but I don't recall whether it was part of a broader computer security meeting or part of the IDA effort that was going on at Princeton.

Yost: Do you know or do you recall if that was the first dissemination of that term and that that was the paper that it was from?

Edwards: I really don't recall. I suspect the early 1970s, you know, 1971 [or] 1972 paper was classified at the time. But the term was footnoted in that particular paper. So it is possible the 1974-75 thing, which I have some memory on, but no details; not a copy of the paper. Nothing in a quick look across the material currently on the internet turned up anything which rang any bells.

Yost: In the early years, after you came up with that, did it really take hold in the computer security research community, or did it take some time for that to be the standard term for that particular vulnerability?

Edwards: Yes, I don't recall another shorthand which developed to describe that particular issue, but then I may be biased.

Yost: I understand that Steve Walker organized a number of meetings in the 1970s that were over at the National Bureau of Standards. Did you attend those meetings and do you recall that set of meetings?

Edwards: I may have attended some of those. As I recall, a lot of those had to do with the notion that some form of cryptography needed to be made public, such that people could protect their information. But NSA, obviously, had a proprietary interest in making as little information available such that some of the other activities that went on at NSA would not be impaired. And there was a lot of back and forth, essentially; tensions.

Yost: Some of the early discussions that were kind of prehistory to DES.

Edwards: Right. But then again, a lot of those were more on the mathematical side, not the practical or other programming stuff, which I tended to be involved with. So I was aware of some of the discussions but certainly didn't participate in the decisions that were made.

Yost: And in the early 1970s, you were on the Anderson Committee. Were there other areas of computer security you were working on in the first years of the 1970s?

Wright: Nothing particularly comes to mind.

Yost: And what about the mid- to later 1970s?

Edwards: The thing that comes to mind — and I don't have specific sorts of dates — is the creation of the National Computer Security Center at NSA. The C organization had

turned into T, Telecommunications, but they were still running all of the wonderful stuff in the basement. The letter "C" was open and so the C organization was formed, trying to bridge the gap between what was going on behind closed doors at NSA and the general public. Or more specifically, computer vendors whose systems we became more and more reliant upon, and the notion that security would have to be built into those particular systems became quite clear because NSA really didn't have the talent, manpower, whatever to completely write their own operating systems. We would be definitely beholden to things provided by IBM, and Honeywell, and other vendors. And trying to get these other vendors onboard meant that they needed to be aware of what the problems were. Trying to bridge that gap was the mission of computer security organization.

Yost: So, going back to the 1970 Defense Science Board Ware Report, one of the key points of emphasis at the end of that report is the need to keep computer security research open and the need to partner with industry. And was there a sense that really wasn't happening and that was part of the impetus of the National Computer Security Center, that there needed to be greater incentives for industry?

Edwards: I believe that was part of that. The natural penchant inside NSA with respect to open versus closed certainly shaped the thinking in the late 1960s, early 1970s. How much can we say? Who has a need to know? But I think it became…

Yost: So was there a sense at NSA early on, at least among some, that things needed to be developed internally so that they'd have control over them, versus…

Edwards: Yes, there was clearly that sort of tension within NSA.

Yost: But over time, there was recognition that it's simply not possible for NSA to internally produce operating systems for all its computers, am I understanding this correctly?

Edwards: Right.

Yost: Something that I found very interesting in the interview with Roger Schell is that he said that it was his thinking, and I think that he also was expressing the thinking of some other colleagues of his, as well, but the one place that the National Computer Security Center couldn't be or shouldn't be, was NSA because they have a fundamentally different view of the computer security problem. He of course became associate director of the center. But was it your sense that there was a different perspective? You mentioned that there was a need for multilevel security even at NSA, but I guess Roger saw it as not comparable to what was truly open systems existing in the Air Force and DoD environment outside of NSA. Can you comment on that?

Edwards: I guess the notion of the openness was one of the things which was really a tension within the NSA community at that time. The projects that we were involved with, as far as the early research, were classified. The examinations that we did with some of the early Tiger Teams were not things that we wanted in the *New York Times*. And you

also had sort of the internal part of NSA where the two missions of NSA clashed with one another and the notion of this third thing, computer security, which wanted to be open was yet another piece of the culture was not immediately accepted with open arms.

Yost: So was there a different sense of what was needed within the computer security research group — you and your colleagues in that small group — than from NSA more broadly?

Edwards: I believe that to be true. I think some of the early suggestions were that the Computer Security Center should be a branch of the communication security part of that. But within the computer security community that was strongly resisted because of the classified nature of the communication security task. We didn't really see how the openness part of computer security community could be carried out under the supervision of the communication security organization.

Yost: So Schell's, and perhaps other's, vision of the potential conflict was likely because of the far larger and I guess more powerful COMSEC side of NSA versus the computer security side where interests were more aligned.

Edwards: Yes. I recall that as the Computer Security Center was initially put together, we were aware of the challenges with respect to this tension within NSA. And part of the thinking there was that we probably had 10 years as an independent organization within NSA before the computer security task would be subsumed by another part of NSA.

Yost: So there was a sense that things might change and that this group that was quite different would not continue to exist as it had been.

Edwards: Would not continue to exist in that form in perpetuity.

Yost: Roger Schell thought that Admiral Inman was a major force at NSA, beating out the efforts of the National Bureau of Standards for the center. Is that something that you agree or disagree with, or do you have any comment?

Edwards: I was certainly many levels below Admiral Inman but believed that he was a significant spokesman for keeping that Computer Security Center part of NSA rather than the tension of putting it over with Dennis Branstad and friends over at the National Bureau of Standards. There was also, again, the need for NSA to take some of the principles that were involved in computer security and have them incorporated into systems that were designed there, particularly on communications security side of the house. So I think that was probably one of the reasons why in the back and forth between NBS and NSA, NSA was finally tasked with putting together the Computer Security Center.

Yost: Do you recall if Steve Walker had any role with this, and if so, what it was?

Edwards: I don't have specifics on Steve Walker's role, but he was certainly a force to be reckoned with in terms of the political discussions that were going on back and forth. And his position was sufficiently high such that things that Steve had to say were taken seriously and had to be accepted or good arguments put forth to say why they were not being accepted. Trying to knock heads together, essentially.

Yost: Certainly, the rather all-consuming and principal task of developing criteria that became TCSEC, or The Orange Book, was the force behind the creation of the center, but was there a sense that at the formation of the center, that that was one principal task and that the center would also work on other things besides that work on developing standards and criteria?

Edwards: I think standards and criteria were seen as only one part of the task, and technical research as to how you were able to carry out the things that we wished we had, was another important part. Let's see, we had C1, C2, C3, and C4, as I recall. I was certainly much more focused on the C1 side but had regular contact with folks along the other part of the Computer Security Center. Mel Klein was brought in to be the initial head of that. One of the things which he tried to do was reach out to partner organizations and other places around the world to bring them on board with computer security. I remember taking a trip to Germany with Mel Klein to talk with some of the folks over there about computer security, and the challenges, and what we thought needed to be done.

Yost: Were these computer security researchers within the German defense or intelligence community, or outside of it?

Edwards: They were part of the intelligence community.

Yost: And do you recall if your ideas and notions of what was needed were similar to or different from theirs?

Edwards: My impression is that the things we were talking about had not really found a way on to the radar screen of the folks that we were talking to. We were doing sort of basic evangelism kind of work and trying to get the word out about computer security and steps that could be taken to make things more resistant to the kind of penetration, Tiger Team sorts of things.

Yost: In addition to Germany, were other European allies, or other allies outside of Europe part of the evangelistic efforts?

Edwards: I was not personally involved with any of those. I suspect it went on during the trip which I made to Germany, which was some time in the early 1980s. It was the only one I was personally involved with. I was the technical briefer trying to give more details as to what was actually going on, particularly in the standards area because that was the part that I was involved with at that point in time.

Yost: I don't know how important titles were at NSA but did your position change or title change with the formation of the center?

Edwards: I am sure I had a title; I am sure I had a business card, but I'd have to go digging to see what that was. Maybe in the front of The Orange Book, or something like that. Seems to me The Orange Book was purposely mum in terms of who was actually doing the writing, who contributed the various ideas that went into that. It was Sheila Brand, essentially, who was tasked with taking the engineer speak and trying to make it more understandable to people who didn't spend their waking hours thinking about computer security. Sheila was one of the persons who got recruited to work on that particular document.

Yost: The ideas came from a number of people but she was the principal composer?

Edwards: Yes, composer, essentially her draft. She would write things up and other people would read them over and make comments. And it would go around the production cycle for — I forgot how long before The Orange Book was actually published.

Yost: Initially issued in 1983 I believe and reissued in revised form in 1985. In terms of developing the technical criteria for the different levels, can you talk about what organization of labor was established for that task?

Edwards: Roger Schell, clearly had a very big hand in that. I guess I contributed at least part of trying to take the spectrum of threats and break them down into levels that, at least at that time, made sense. I guess one of the decisions was, is A1 the highest? The argument I made was A1 may be the highest that we can think of now but there's going to be progress in that, and leaving the A level open to something better than A1 seemed important. That same idea was carried down into B, C, D.

Yost: And that was the reason things were shifted and A1 became what A1 was; that there may be one or two levels that are recognized in the future that are needed above A1.

Edwards: Correct.

Yost: Very interesting. I wasn't aware of that. Was there heavy debate and were there some fundamentally different viewpoints that had to get hammered out in developing the criteria, that you recall?

Edwards: I guess the whole notion of mathematical provability of what was happening in computer programs was discussed for a long, long period of time. Trying to decide, was this, in fact, possible? Could we actually do that? Was something that went on and on. But since that was sort of the basis of the A level, where we wanted everybody to be, there were a number of discussions that went on, and people came and went, trying to crack that particular nut.

Yost: What was the sense of what was achieved, both your sense as well as others you're aware of, with Bell-LaPadula, in terms of mathematical backing for assurance?

Edwards: I think part of that was looking at the basic framework and then trying to provide a working version of that, and that's what the Ford Aerospace contract was doing with Mike Pliner and friends.

Yost: KSOS?

Edwards: Yes. And the…lack of success — can I say? — in actually being able to produce a system which had the level of mathematical verifiability we were looking at was, I think, an eye-opener. But as that particular research contract went on, the shifts, essentially, in approach trying to write something which was both provable and implementable, really came into pretty sharp focus. So, I guess, one other thing that was part — not part of the contract, but came up as a result of some of the work that was going on there at that point in time — small hand held calculators were becoming more widely available and realizing that those calculators could be programmed and they could be used as part of a two-factor kind of authentication system was a notion which I had. I discussed it some with the folks out at Ford Aerospace and was somewhat surprised that the Ford folks took the basic idea and put together a working implementation of that in a hand held device. And I think they actually went forward and tried to patent or sell that particular notion. I don't recall that being recorded anyplace, but I believe the idea is one that I originated.

Yost: You were sharing ideas to try and develop best practices and they saw [pause]

Edwards: Potential commercial IP.

Yost: Commercial IP.

Edwards: Yes, attribution was not something that I was particularly looking for, but I was still a little surprised.

Yost: Did anyone in the early computer security research community you were involved with ever have any patents or was that considered something that was acceptable practice?

Edwards: I don't recall the idea ever coming up, as to looking for patents and I suspect that was probably an outgrowth of the community notion that we were working on this together and the initial consternation that we would have to have passwords on the Multics system sort of hitting us. Looking back it was perfectly obvious. Corby took steps to apply some very basic computer security, and that was back in the mid-1960s. But I think there was very much a sense of community in working on the various computer security projects that I was involved with as part of the Computer Security Center.

Yost: Far earlier in this discussion, you mentioned very early work — and perhaps the earliest work — the Tiger Team efforts to learn from breaking into systems. What became the most famous early efforts were those that were later conducted by Schell with the Multics Tiger Team effort. Was there any learning that occurred, any knowledge that was developed at NSA that Schell and others learned from in doing the Multics Tiger tests that diffused…?

Edwards: I guess I wasn't particularly involved in the Multics Tiger test and I would have trouble putting on a particular timeline from when Multics was initially put together. But I do know that Tiger Team efforts went on, on classified systems that were both inside and outside of NSA. And results of those tests were discussed in classified settings and the sort of techniques, you know, the things that we looked at, were shared with folks who were involved with that sort of work. So I suspect some of the earliest Tiger Team work that we did inside and outside NSA, at the request of other classified organizations, fed into that pool of knowledge and influenced hardware designs as well as software practices.

Yost: This may be something that you can't comment on, but the learning that occurred in doing Tiger Team efforts were — obviously, there is an intelligence gathering side to NSA. Were those separate people in separate efforts, or were some of the same people on Tiger Team defensive and offensive sides?

Edwards: The only part that I'm familiar with was the part that was carried on by the computer security R&D folks. If other stuff was going on in other parts of the organization, I am not aware of it.

[BREAK]

Yost: I was just getting set to ask you to what degree was industry consulted in developing criteria for The Orange Book and did their input have any significant impact in how the criteria was set up?

Edwards: I think the criteria was basically developed at NSA and briefed to various parts of industry but I don't recall a whole lot of industry input, basically because there simply was not a high degree of awareness of this set of problems or things which needed to be dealt with by the computer industry, at least to the best of my knowledge.

Yost: Was the work for developing the criteria principally done by those employed at the center or were outside consultants such as James Anderson, or perhaps others, brought in?

Edwards: I suspect Jim Anderson was involved. You know, the whole idea of a criteria was essentially evolving over several years. Various Anderson contracts were involved. Discussions with the folks at the National Bureau of Standards, I think, was also part of

that. But it was essentially a standards mission to take this issue and try to put it into a form that could be signed off and agreed [upon] and promulgated.

Yost: Was there a strong alignment of objectives at NBS and the center, or significant differences?

Edwards: I don't recall a whole lot of discussion. That is, I don't recall any strong objections received from the NBS folks, but then I think they were focused on other tasks — the DES and related standards. And where the criterias actually, that we were putting together, seemed to be more focused on defense related things. I'm not sure the NBS folks saw that as something that would be more widely adopted in the federal computer community.

Yost: Speaking of the federal computer community, there were some individual projects like KSOS and Honeywell's effort with Multics that were aimed at — and also at DEC effort under Steve Lipner — that were aimed at high levels of assurance, high levels of security, B2 and A1. But what was actually being put together as products that got widespread use, by the late 1970s were the leading two products that grew out of the 1974 IBM SHARE meeting: that was RACF and a competing access control product, ACF2. Were you aware of those products?

Edwards: No.

Yost: I think over time, after a number of refinements and later iterations, RACF got a C1, after initially shooting for C2, so it wasn't really high up on the level but really, RACF and ACF2 can be seen as IBM trying to listen to its customers. Customer organizations in industry in general were resistant to security that might slow down systems or add expense to systems.

Edwards: Yes. I think that was generally the industry response to the notion of computer security. Again, this is pre-internet and the damage done at one particular system, even if it were a time-sharing system, is still pretty limited and all of that really changed as the notion of computers in different places around the world, all communicating with one another really came into focus. That was still pretty much the ARPANET group. Essentially, the internet hadn't appeared in the general public until much later, but I think you can see the flow of ideas from some of the early computer security thinking. Again, I think Roger's big contribution to the whole x86 architecture in being able to really virtualize the machine, which made the notion of a security kernel doable, had an influence that has persisted for decades.

Yost: Were there principal parts of The Orange Book that you were most heavily involved with or was it just involvement with all levels of the criteria development?

Edwards: I was involved across the spectrum, since I had some experience on the Tiger Team side of it, as we were thinking about the various kinds of attacks that we could foresee, wrestling, again, with how far can we push the provability. We've written a set

of verifiable specifications and we can prove that this code matches that set of specifications was all part of the thinking that went into that.

Yost: So you were principally involved, Roger was, Sheila . . .

Edwards: Yes. Sheila Brand.

Yost: . . . Sheila Brand drafted The Orange Book. Were there other people that had a really large role that you recall?

Edwards: No names particularly stand out at this point, but the whole notion of community going over; I suspect Marvin Schaefer had some good things to say about the various contractors that we looked at. I don't recall Peter Neumann involved in this particular thing, but I suspect Clark Weissman had input. So I think, within the computer security community, there was a fair amount of input that went into that. It certainly was not an NSA C1, here it is like-it-or-lump-it kind of effort.

Yost: As it was being developed, did you think that industry would embrace it more as an incentive to get certified? That such certification, while not a huge market, was a large enough market that it was a proper incentive to get them to invest.

Edwards: I don't recall many discussions along that particular line. I see it as an attempt to write down what we thought we wanted and then try to sell industry on delivering something which would meet this.

Yost: Was this driven by the needs of the agency, and the defense and intelligence communities?

Edwards: Yes. Again, the applicability of any of this to general accounting, CAD, and all of the other uses of computers at that particular point in time, certainly was not central in my thinking. I think it was driven primarily by what the defense department and other intelligence groups needed to be able to enforce the notion of "need to know."

Yost: I assume that you attended the National Computer Security Conference on a regular basis, is that correct?

Edwards: Yes.

Yost: Was that used as a forum to get feedback and ideas for The Orange Book?

Edwards: I think the computer security conferences were mainly presentations. I don't recall a whole lot of discussion or feedback coming from the computer security conferences. That is, it was pretty much of a push or effort on the part of the C organization trying to get industry folks in to hear what we were saying. But I don't recall

a lot of interaction with industry representatives based on the sorts of things that we were presenting there, other than, again, the defense and intelligence community, and their contractors, essentially, who clearly had a much bigger vested interest in doing things which keep us happy.

Yost: The IEEE Computer Security and Privacy Symposium was launched in 1980. Did you attend that first event or did you attend that conference in its early years?

Edwards: I don't recall. If I did, it didn't make a terribly big impression on me.

Yost: Is that a conference that you went to somewhat regularly over time, or not?

Edwards: I don't think it was.

Yost: I get the sense that there are some people that overlapped and went to both, but many others, especially people in the defense and intelligence communities in the D.C. area, the National Computer Security Conference was their main conference.

Edwards: Yes. That's the one that I clearly remember taking part in. I was emcee at one of those, as I recall. And I simply don't recall a lot of interaction with the IEEE security and privacy folks.

Yost: Some computer security pioneers we've talked to have mentioned that there were different factions or kind of world views of how people saw computer security. Is that a characterization that you would agree with and do you see yourself having a particular identifiable vision for computer security?

Edwards: I guess I don't particularly connect with that particular set of notions.

Yost: One of them is kind of a high assurance group that Schell himself I think has identified with. He really embraces high assurance and provable systems, and others characterized him as high assurance being really the — I don't want to put words in his mouth — but the only real computer security that truly matters, what is truly needed. Whereas others, for instance, Steve Lipner, who was at MITRE and DEC, was involved with high assurance work and now works at Microsoft. They're certainly not developing A1 level systems at Microsoft. Perhaps it could be said that he's taken a more pragmatic turn to, well what can we do that has some real world influence versus mathematically proven high assurance.

Edwards: I guess I'm thinking that the high assurance approach was sort of the gold standard. There was, at least, optimism at the beginning of the effort that something like that could be achieved. As time went on, the difficulties in actually doing the high assurance stuff in practice, I think more people were able to grasp. So pushing for the ideal but also understanding that very few systems were actually going to make the ideal. And we needed a spectrum — you know, the A-B-C range rather than simply put all of

our eggs in the A-level basket — was all part of the thinking and discussion that went on in the late 1970s or late 1980s.

Yost: In 1985, you left NSA for what I think you termed in your email, a second career.

Edwards: A second career.

Yost: Can you tell me a little bit about that decision and what you did?

Edwards: Let's see. I guess, in the late 1970s I was thinking, you know I was getting a little bit tired of engineering and wanted to see whether I could do something in management. The management opportunity came along with the Computer Security Center and my position as leader of C1 [one of the four divisions of the C (Computer Security) organization], that turned out not to be a whole lot of fun for someone who is basically an engineer at heart.

Yost: Your position as . . . ?

Edwards: As manager. I guess I'm much more of a hands-on.

Yost: So when you refer to C1, that's manager of that group?

Edwards: Manager of that group. So I actually took on part of a project that was internal to the NSA, which was focused on delivering end-to-end encryption systems, and did some of the architecture work associated with that. [I] was actively involved in overseeing the contracts that were building the equipment to realize that particular vision. I was involved in that for several years in the early 1980s, and also in the early 1980s, I was exposed to the idea that my computer skills could be used in other areas. And I had a desire, essentially, to set aside the computer security career which I had done up to that point, and pursue some of these other opportunities to use computer skills in the area of bible translation. So in 1985 or so, I resigned from the agency. This was a point in time when our youngest child, our son, left home to go to college. That looked like a good time to give up on the government side of the career and do some hands-on work in supporting the work of bible translation. So, dropped our son Jonathan off at school, sold the house, moved to Waxhaw, North Carolina, to start working on computer programs at a completely different level than computer security and program kernels and penetration testing, and all that sort of stuff.

Yost: Was that something that you did with an organization? Did you consult?

Edwards: It was essentially a personal decision, which got involved with the JAARS organization, which at that time stood for the Jungle Aviation and Radio Service which is the technical support arm for work with bible translators. Some of the software that they were developing I found interesting in terms of being able to use simple computers to do linguistic translation kind of work. So I did work there and managed the software

development in Waxhaw for a few years and then took a position overseas. When retirement time came up, you know, I retired from that, but the word retirement isn't in the Bible and additional opportunities opened up for us to be involved overseas. At this point in time we spend about seven months every year in Chiang Mai, Thailand, on providing computer support on several projects over there and having a blast.

Yost: Terrific. Looking back at the history of computer security, do you see any major missed opportunities or paths that might've been taken that weren't that could have had a fundamental impact?

Edwards: I think the thing — well, let's see, let me back up. I'm basically an engineer, okay? And not the kind of strong leader which is necessary to get things done in the real world. I think the engineers play an important part of that but without the skill and leadership of folks who are much more people-oriented important things tend to fall in small holes and never see the light of day. The tension between the classified side of the world and the bigger picture, I think constrained getting the notion of computer security out. The other thing that was just totally missed during the time that I was involved in computer security is the sea change invoked by the network. The challenges imposed by having hundreds or thousands of computers all talking to one other across the network and the impact that that would have on the whole security picture just didn't break threshold. I suspect that is probably one of the biggest things that was missed: being able to focus in the early days of the networking and foreseeing the challenges that would be faced there, and building into some of the basic mechanisms things which could be used

to mitigate some of those challenges. You know, the original worm that Bob Morris' son released at Cornell was a real wakeup call. I remember hearing about it and essentially understanding what happened, and saying wow, we have missed it — in terms of being something we really need to be paying attention to.

Yost: And from what I understand with the principal people involved with the ARPANET and its evolution to the internet, security wasn't given much consideration at all.

Edwards: I guess Vint Cerf would be a better one to comment on that than I am, but my impression is that security was not high on the design criteria. And I'm almost afraid if security were high on the design criteria, the network may have been delayed for decades. So the balance between openness and security is a tradeoff that needs to be continually assessed and reassessed moving forward.

Yost: And finally, are there any questions I didn't ask or topics I didn't cover that you would like to discuss before we close?

Edwards: Nothing immediately comes to mind. As I say, I've been out of the business for 35 years now.

Yost: Thank you so much for taking the time to be with me this morning. This has been extremely fascinating and helpful.

Edwards: Thank you for taking the effort to come and find me. [Laughs.]