An Interview with

TERRY BENZEL

OH 457

Conducted by Jeffrey R. Yost

on

18 November 2014

Computer Security History Project

Marina Del Rey, California

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

Terry Benzel Interview

18 November 2014

Oral History 457

Abstract

Computer security pioneer Terry Benzel discusses her education and programming work at Charles Draper Laboratory, before focusing on her work at MITRE Corporation, Trusted Information Systems (TIS), Network Associates and USC Information Sciences Institute (ISI). The MITRE discussion highlights her early role and perspectives on criteria evaluation (including her role in the SCOMP evaluation) in the formative years of TCSEC and after the publication of the criteria in 1983. Starting as a TIS principal scientist she rose to become a vice president in charge of the West Coast (Los Angeles) office, and later led a research team of 120 scientists/engineers for Network Associates. Among the technologies discussed are firewall development, and the security testbed at ISI.

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

Yost: My name is Jeffrey Yost, from the University of Minnesota, and I'm here today at ISI (USC) in Marina Del Rey, with Terry Benzel. It is November 18, 2014. Terry, I'd like to begin with some basic biographical questions. Can you tell me when and where you were born?

Benzel: Okay. I was born in Lansing, Michigan in 1956 on November 17. I had my birthday yesterday.

Yost: Happy birthday.

Benzel: Thank you. But I moved around quite a lot, I didn't stay there long. My father was in graduate school at the University of Michigan; [he] finished his master's there, then went to Stanford University for his Ph.D. We moved a lot.

Yost: Can you describe yourself as a student in your pre-college days? What were your interests?

Benzel: I fell in love with math in the sixth grade, in Laytonville, California. I lived in a tiny town in Mendocino County, I mean, like the population of the town was 900 people. My father is a philosopher logician, and so I grew up with these yellow legal tabs with logic scribbles on them and I was always very interested in that and wanted to see it. He

actually came in and taught a logic class in my kindergarten at Peninsula Elementary School in Palo Alto, out here as a Ph.D. student. So I was always exposed to math and logic and had a love for it. And then I truly remember Mr. Christensen's class in sixth grade, in Laytonville, California. A real backwater, backwoods place in the early 1960s; actually living on a commune, a bunch of hippies on a commune. But Mr. Christensen loved math and loved teaching it to students. And we actually, in sixth grade, studied geometry and he had us sew cardboard pieces together to make geometric shapes. He taught us a little bit of basic algebraic proofs and all the concepts about distribution and equality. I just remember saying now this makes sense to me; you add on this side and you subtract on this side; and wow. I vividly remember that, so pretty much from the time I was nine or ten years old I wanted to study mathematics. I bounced around. My parents were divorced I lived with my mom up on that commune, and then when I got to high school age my father brought me down to Laguna Beach in Southern California to be in a high school that was more rigorously academic. I did get to college. Both my parents were academics; I grew up in that orientation. I was a little lost in high school from moving around and being a new kid. I showed up in Laguna Beach and I was the only kid with brown hair and everybody else is blonde hair and surfing. So socially, it was a hard time for me but I always just stayed with the math and loved the math. I had some really good teachers there in high school and I again, sort of had some difficulties socially and struggled in the 1960s and 1970s. I ended up actually starting college at a community college in the Bay Area, Los Altos Community College. I turned down my acceptance at UC Irvine to stay with a boyfriend. And there I had an amazing teacher, in a community

college, who saw my love of math and gave me the opportunity and I proved Gödel's Incompleteness Theorem my freshman year of college. I really had someone who wanted to work with me on that. Then from there I went to UC Santa Cruz, again based on social situations and near a boyfriend, etc. Santa Cruz wasn't really the right place for me. They have an excellent math department but it wasn't in the areas I was interested in. And then again for social reasons, I went to Boston University, and there I found my home again and started working for a Ph.D. in abstract algebra. Going back to that first flash of algebra, that algebra is the answer to all problems. [Laughs.]

Yost: Were you still an undergraduate when you started working at the Charles Draper Laboratory?

Benzel: Yes, when I moved to Boston I got a job at Draper. Actually when I moved to Boston I got admitted into a joint undergraduate BA/MA program, and then applied from the MA program into the Ph.D. program. To earn money while I was in school, I got the job at Draper. I had also — backing up a little bit — when I was in high school in Palo Alto, I had gotten a job at NASA Ames Research Center and I have to say that really set my career in science and research. We worked on the space shuttle. We had a one-third model of the space shuttle before it ever flew. This would've been 1973, 1974, somewhere in there; and I worked with basically job control language on these big, huge mathematical simulations of wind and lift on the space shuttle. Just a great place to work. So when I moved to Boston and looked for a job, I naturally gravitated toward another

research laboratory and I've been in research labs ever since. Shall I go on or do you want to ask a question?

Yost: I was just going to ask, the research that you did at Draper, was that connected to your master's thesis?

Benzel: Yes, when I first started at Draper, I was just a programmer. But then when I got into grad school and started doing a master's thesis, I looked to see if I could do a directed study at Draper. You know, allow myself to make some money; I didn't have a graduate fellowship at that point. And Draper at that point was working on the F-15 and we were looking at image processing algorithms. So the plane flies, it tips its wings and takes pictures, and does "friend or foe," you know. So my thesis was the parallel processing algorithm to get better than one over in performance on those algorithms. Fairly standard kind of stuff. But I was able to work with the engineers that were doing the engineering formulas and the analysis of it, and develop a set of algorithms, do a performance characterization of it, and write my master's thesis. And then I stopped at the master's thesis; I did not go on to a Ph.D. program.

Yost: Can you talk about important mentors at that stage, either at the lab or at Boston University?

Benzel: Yes. You know, at the lab, it was good support there, but again, I was a little on the edge because most of the people there were M.I.T. students. I was over on M.I.T.'s side of the river, not at the BU. So I don't feel that I was quite as enveloped in the environment. I would say at the BU, Harvey Deitel taught an operating systems class, and that began my interest in computers, and moving me a little bit away from mathematics. I really enjoyed that operating systems class, and took more advanced operating systems with Harvey Deitel. I have the book I still reference all the time; it's an IBM-published monograph on operating systems. And in fact, he used many of our graduate student papers as input into that book. So it was also another place where I got a first cut at how to do research and publish.

Yost: How did you end up on the technical staff at MITRE? You had enrolled in the Ph.D. program but had a job opportunity?

Benzel: [Laughs.] That's a great story. I was in a graduate student symposium seminar class and we were reading journal articles. There was a journal article — Cheheyl, Huff and Gasser — on proving programs correct for security. It was in ACM *Transactions*, I believe. I read this in the seminar class and it was just a light, I just lit on fire because there it was. It was mathematics, it was proof, it was logic because proving proofs is more logic oriented than algebra oriented, and it was computers. That was it. At that point, I really wanted to get out. I wanted to have a life; I wanted to make real money. I didn't want to stay in graduate school. And the paper was written by these people at the

MITRE Corporation. I'm in BU, right? And then, as it turns out, my then-husband — or I guess we were engaged at the time — his best friend worked at MITRE. And so his best friend, Dan Moulin, said to me, they're having one of these employment fairs on Wednesday night, why don't you come by? I walked into the employment fair holding this journal article and I walked up to the first person I saw and said I want to do this. They were so excited because at that time, computer security was a really small field. This would've been 1981-ish kind of timeframe. Very few people knew, or understood it, or appreciated it. So pretty much it was a love fest from then on. I met those people that night, they invited me in, I went to an interview. That was like November or December and I wasn't scheduled to finish my — now that I had decided to do a terminal master's, I had to finish that — and I had 'til May or June to finish the terminal master's. So they hired me in January and gave me three raises before I started in May. [Laughs.]

Yost: Great!

Benzel: So I started in May of 1982. That the right year? I don't know. You have the year, probably.

Yost: Was the SCOMP evaluation project the first major project you worked on?

Benzel: Yes, I think that was pretty much the first thing I was put into because I came in there saying I wanted to do program verifications. And they didn't have a lot of people

doing that at the time. You know, Cheheyl, Huff and Gasser had written this paper that was on the theory of it and how it should be applied. It was arriving at the right place at the right time. SCOMP work had been going on, evaluations were just getting started, a TCSEC hadn't been finalized yet, Grace Nibaldi had the green cover of the TCSEC at that point in time. They said we hired this person who's interested in that. I very quickly became the leader of the formal verification team that worked with Honeywell. Honeywell did the actual verification, as well as two Air Force lieutenants that were assigned to the NSA. But I ran the evaluation team that analyzed that work.

Yost: Can I go through some of the people involved and relate what you remember about what they did?

Benzel: Okay.

Yost: So at Honeywell, John Silverman and Chuck Bonneau?

Benzel: I worked a lot with Chuck Bonneau. When I went back and looked at that paper this morning to kind of prep for this discussion, I didn't remember Silverman; I can't place him, *per se*. I certainly did work very, very closely with Chuck. He was a mentor; he taught me a lot. It really pulled forward that interest I had in operating systems that I had learned in grad school. I had this book and I had really studied operating systems. But working with Chuck, who wrote the code for the operating system; he was a key

developer of it as well as working with the verification team. It was great because there I was, living in this code, it's 20,000 lines of code for the operating system, and then all the formal specifications. I'd been, in a sense, reading logic since I was in kindergarten and this was just great. And then I had operating systems. So Chuck Bonneau was a great mentor and a wonderful person to work with. Another person that you might not have run across would be Carl Landwehr. Carl Landwehr was at the Naval Research Labs. It was so great. I still work with Carl. I was just at the IEEE meeting with him on the board of the Computer Security and Privacy magazine, and he was at your workshop.

Yost: Right.

Benzel: It's so great to keep working with those same people. So Carl was at Naval Research Lab and had a role — I don't know what his formal role was but I know he was at all those formal verification meetings, so maybe some of his staff was helping to support the verification.

Yost: And Harvey Epstein?

Benzel: Yes. I'm glad I did a little reading this morning before we got together — yes, Harvey was at MITRE, much more senior than I was. He helped guide me through how to participate on a team as a MITRE person, and he really had the deep insights on the

tool from the verification tools, much more than I had the opportunity as a first year member of the technical staff.

Yost: Dave Drake?

Benzel: Dave Drake was a colleague; he worked with me on the team. He too had a background in math and was interested in formal methods, but he was young like I was, I mean, we were just a group of young people that were interested and excited about this. We worked long and hard hours on it and it's really tedious stuff. I looked back at this morning and I thought 'ugh, how did we do that?' And then the two guys from the National Security Center at NSA were Grant Wagner and Todd, Tad?

Yost: Tad Taylor?

Benzel: Tad Taylor, yes, right. I still see Grant once in a while. He's still there at NSA. I don't know quite what his position is exactly, right now. So, it was really collaborative. Later we're going to talk more about how the evaluation became adversarial in certain situations, but at that point in time, we were really one tight, collaborative team. The two guys from NSA who came in helped take over getting the verification done. And that's talked about in that paper you referenced, where there were two major theorems that needed to be proved and Honeywell threw up their hands and said this is taking a lot of time. The two guys from NSA took over cranking those through the theorem prover

while I set up the analysis aspect of it with my team, which had Dave Drake on it. I vividly remember, we spent like a month locked in a conference room at MITRE where the guys from NSA came up, and me and Dave and I think had a few other people locked in a room with the formal verification tools, the specifications, their output, the code, the data, Dan's specifications that did that code-to-data mapping, which I pretty much came up with, along with Kim.

Yost: And this was the first verification at the A1 level. Was it the very first?

Benzel: Yes, it was the very first system to be subjected to an A1 evaluation and we started the evaluation before the TCSEC was completed. Later, SK VAX out of DEC, with Steve Lipner leading that, came along as the second A1 but SCOMP was the very first one. It's almost — I don't quite know the politics or the funding — but SCOMP was built to prove out the TCSEC A1 requirements so that's why there was a lot of synergy back and forth between the two, and not quite as adversarial as later evaluations happened.

Yost: Had there been any evaluations for lower level systems prior to that, and was there any learning from those?

Benzel: I believe what happened at that time, both MITRE and The Aerospace Corporation were doing the evaluations. My memory is there was an attempt by the

National Computer Security Center to choose a candidate for each level as a way to test out the TCSEC. So there were some C1, C2 evaluations, which I think were primarily let out of The Aerospace Corporation. There was a B1 evaluation, that I might've had a little bit to do with. There was the Amdahl project that was going for A1 level. So there were a range of evaluations that were going; all getting started during that formative year on that. I do think it was some of the lower level ones that started raising the interpretation question — how do I interpret this? It's interesting that the interpretation first came to light at what you might've thought would be straightforward mechanical issues: how do you evaluate discretionary access control? Is it an AC or an ACL? How do you satisfy that? The issues at a higher level that later became big issues had to do with modularity and software engineering at a much more abstract level. So they were pretty night and day, in terms of interpretations. And in a sense, we on the SCOMP team had the advantage that we went in sort of assuming those higher level properties. Obviously we could not have gotten to the place of doing a verification if it wasn't modular and well-specified and abstract at the right levels. I think things in the B1 area; B1, B2 started having requirements for modularity but you didn't have as clear cut a way of evaluating that. And also, for something like the SCOMP, it's only 20,000 lines of code in Pascal. So you're in a higher order language already and it's 20,000 lines of code. I mean, any of us can read 20,000 lines of code; and it was modular and it had multiple levels of specifications. The B1, B2, RACF added on to an IBM system. You know, the IBM system itself, millions of lines of code. And even the RACF system, right? What's the

interface between this thing added on and it's like well, much harder problems, actually, than on at the top level.

Yost: Were there instances where the ongoing work on the SCOMP or by the SCOMP evaluation team influenced how TCSEC was written in 1983 versus what was in the Nibaldi Report?

Benzel: Yes. You know, I'm sure whether or not I can dig up a specific example. [pause] I think that modularity — I'm going to keep coming back to that because I think I remember that's the one we had the most discussion on. And I think that the Nibaldi Criteria also had some requirements on modularity and code to specification that turned out to be more strenuous than what ended up in the Orange Book. So, generally, my memory of the changes between the Green Book and the Orange Book was there was a slight lessening of some of the requirements. And that makes sense; I mean, you're going to write a criteria and you're going to write it as stringent as you can but once you start working in the real world you have to loosen up the corners a little bit. And all this interpretation process, 90 percent of it was oriented towards how do I make it adapt to reality? In a few cases, there were, in my opinion, cases where people went overboard but I'm not going to nail them on this. That's not productive.

Yost: Was there much involvement of individuals in the top leadership of the National Computer Security Center, like Roger Schell?

Benzel: Yes. [Laughs.] Everybody was so interested in part of this and I remember, you know, we had a problem with proving a certain aspect of Bell-LaPadula in the SCOMP evaluation and in the formal verification. There were a number of instances that I described in that paper, right? I've never been shy and always a little bit aggressive, and I spent hours arguing with Roger Schell at the Computer Security Center about how we should be able to evaluate this. ***Huge*** learning experience. I mean, I thought I knew the answer and I was in there literally week after week, flying from MITRE down to the Computer Security Center, sitting in Roger's office. Marv Schaefer was there at that time, too. You know, sitting in these guys' offices who were like the leaders of that whole community and I'm 24 years old, right out of graduate school. I learned so much. And of course, Roger was right and I was misguided in the argument I wanted to have, but it was a great learning experience to have the debate.

Yost: And what about Dan Edwards, was he also involved?

Benzel: You know Dan was quite involved, more from a management point of view. He's a fairly quiet observer kind of guy. So he would show up in our meetings but really, when things got heated and hard decisions had to be made, he pretty much delegated that either to Marv Schaefer as chief scientist or Roger. And Marv was probably the most involved on a day-to-day basis, then Dan. But certainly, we had access to all those people

and we spent time with them, and they sat in our meetings. It was a very actively involved environment for everybody.

Yost: In 1983, Lester Friam of Honeywell Information Systems published an IEEE *Computer* article on SCOMP. What was your reaction to the article at the time, and his characterization of the system?

Benzel: Well, Les was the manager. Chuck worked for Les, is my memory. Yes, I remember this article now. Sorry. Yes.

Yost: Were you surprised to see this article on SCOMP in one of the flagship computer science journals when a lot of computer security work was kind of behind the scenes?

Benzel: No, because that's the thing. For all of us working on it — here's a relationship between the Navy, right? The Navy, which is where Carl Landwehr is involved in it. This one is the first one out and it was so exciting, so in some sense, looking back, that perhaps my objectivity was co-opted because I felt like I was part of the team building the SCOMP. And so I was very happy to see this article. In fact, it was even helpful from an evaluation point of view because one of the problems you have when you're doing evaluation is when you go in, you don't have a 10-page overview of the system. You're just faced with mounds and mounds of documentation and code. This was a nice, elegant, high level, generally accessible description of the SCOMP and I totally believed the

things that were in here. You know, that was the whole breakthrough with the evaluation criteria and with the National Computer Security Center. When I entered into it, we weren't in the classified arena, and it wasn't in the secret arena. That's what the National Computer Security Center did was brought it all out into the open and created communication with industry and created an industry/government connection. So it was a strange disconnect that you would go into the National Computer Security Agency, which of course has all this top secret stuff. Back then, I don't even know if there were signs where we went. We went to the annex, whatever that meant, right? But then we had all this openness with industry.

Yost: At the time you were working on the SCOMP evaluation, did you have high hopes for industry adopting high assurance systems?

Benzel: Yes, when I first started on it I had high hopes that program verification was the answer. Like I said, it was the solution to my world view. I loved operating systems and logic and what would be the better thing to do. Intellectually, I believed the security properties were simple enough and well enough specified that we could do verification. Certainly at that point in the 1980s, program verification was only seen as working on toy systems to do total verification, but to verify security properties seemed quite relevant. And, you know, it seemed like such an exalted level to go to that all of industry should pursue it. On the other hand, it didn't take long to begin to understand that the market for these kinds of multilevel secure systems was quite small. You later see that, and you hear

*Revised to correct KVM, p. 17.

that from Steve Lipner on DEC, and SK VAX, there's no market to justify the expense that was involved. And we saw that some with IBM and Amdahl; Gemini Computers is another A1 we haven't touched on. But by my early 20s, the purity of it was what I was concentrated on rather than the market forces. It took me a while to understand those kinds of concepts.

Yost: I understand a few earlier systems, KVM 370, long before KSOS 11, that in trying to implement security design elements it significantly impacted performance. Can you speak about that? Were there significant tradeoffs or was that mitigated more with —

Benzel: Yes, that's another thing that was great about being at the MITRE Corporation because there were the people that had been involved a lot, like Marv Schaefer with the National Computer Security Center, but he had a lot to do with KVM, right? And then Morrie Gasser, and Earl Boebert had to do with KSOS, and Peter Neumann; so I was around all those people and had that opportunity to learn from those histories. Performance was a real concern. SCOMP took a different approach. Certainly, KVM is really a virtual machine, on top of the full IBM operating system so yes, it had performance issues associated with it. KSOS tried to apply a 33-bit extra tagged architecture. That has different performance characteristics. SCOMP had a specialized hardware module and felt that they had taken an architectural design that allowed them to not hit as many performance barriers. What ended up, the trade-off, and what ended up with SCOMP — and it was a disappointment to me when we finally got there and had the

thing running — is it basically had no user interface or application interface. They had the SKIP; you really couldn't do anything with it. So the other systems had erred on the side of giving you a full application interface but had significant performance tradeoffs. This went to a very sleek, small kernel, with a hardware assist, but didn't invest the energy in building out the top level. Now you know, jumping way ahead at Trusted Information Systems, you had Trusted Mach, which really was a first case that tried to take a small secure kernel, which is the Mach operating system kernel, and build a trusted application layer on top of it.

Yost: Can you describe the hierarchical development methodology multilevel security tool and its use?

Benzel: HDM was originally developed at SRI, I believe, and it consisted of formal specification language and a theorem prover. The theorem prover might've been based on Boyer-Moore. Yes, it's the Boyer-Moore Theorem Prover. And so it had two stages. You write the specification, then you can run the specification through basically a parser that's able to do a quick analysis. It looked at flow control essentially, and was able to eliminate a certain number of cases where flow control is obeyed, and then flag the cases where things weren't obeyed, and then you process that through the theorem prover, which was a fairly manually intensive effort to make the theorem prover prove these theorems because you had to step it through it. Now, as I say, most of the actual work of running

the theorem prover and writing those specifications was either done by Honeywell, or supported by the guys at the National Computer Security Center.

Yost: I understand that of the 12 covert channels that were identified by the tool, I'm assuming that that's considered rather low.

Benzel: [Laughing] Yes.

Yost: Did that cause questioning of the usefulness of the tool?

Benzel: Certainly on the part of the people in the industry that had spent so much time doing that. If you talk to Chuck Bonneau after he came through all of that, he certainly felt that good software engineering, and specifications, and good understanding of the system on his part found everything that needed to be found. I think if you go back and look at that paper I wrote, I think early on, I and my colleagues were still in the mode of trying to justify the work that we were doing. And I think we say things like well, if you'd really specified it right from the start, and really run everything through, it could've found all 12. You know, that was a lot of our belief was it could have and it should have, except for these contingencies. So I think we still felt pretty good about it, at that point in time. Later, when we finished the mapping of the specifications, you have this formal specification and then you have this code and you're going to map them together; I said that labor intensive effort that we did, right? Something I think didn't

come out in the paper because it was discovered after I published the paper, but when I made the presentation at the conference is after all of that is done, Chuck Bonneau was looking at the code to check a bug that had come up — not discovered anywhere in any of the formal work whatsoever, but somebody said there's a bug — and he went in to look for this bug, and he found a fatal flaw. I mean a huge security hole. Not a covert channel, a flaw in the system; it was a very deep nested clause and that basically left a data segment wired in read access for a low level process; the very thing we're trying to prevent in that system. I had done this code spec mapping and thought we would have caught those things but it's a manual process and humans are fallible. It was deeply nested, we didn't find it. As soon as Chuck called me and told me about it I immediately went into the formal specification, went into the proof. It had been miscoded. Again, all those opportunities to mis-characterize it in all these different layers, so it had been mis-coded in the formal specification, wasn't caught by HDM, and was a complex method statement that we didn't catch in the manual. So, there's Chuck saying I know the code, I wrote the code, it's 20,000 lines, I wrote every line of it. Yes, he missed it the first time through, but he found it and nothing else had found it. And he wasn't looking for it, he was looking for some other bug.

Yost: Did the nature of manually finding things such as that, and identifying seven or eight of the covert channels without the tool, call into question at all whether a system could truly achieve high assurance.

Benzel: [Laughs.] No, I don't think so. It was still many years when we kept pursuing SK VAX and Gemini. I think that well into the late 1980s and 1990s, the community was still in search of the perfect MLS secure system and we should just do a better job of writing specifications and modularity, and we should write new tools to do code spec mapping. I think the DEC team and VAX put a lot of energy toward that; Sue Landauer worked on that at that time and put a lot of energy into how to make it perfect.

Yost: Can you discuss what types of documentation that you did in order to develop methods that could be used on future evaluations?

Benzel: We at MITRE were required to write a number of MITRE technical reports. I still have them in my storage shed; my husband keeps wondering when I'm going to throw them away. [Laughs.] Of the MITRE technical reports that we wrote that described our process, you know, any automated tools that we built, basically things like grep lent and such, to be able to dig through the specifications. Being part of the MITRE evaluation team, we were expected to do a fair amount of documentation. We also did a certain level of training because there's really nothing like experience. So when the Gemini team was started up, and that was run out of aerospace here in southern California, I came here to California and spent time with them, training them on how I had proceeded.

Yost: You mention later on evaluations becoming more adversarial. Was that after the SCOMP project or was that later within the SCOMP project?

Benzel: Well, later within. I mean, one of the first things you have to say about evaluations is that they took a lot longer than anybody wanted them to take, right? And that also starts to call in the whole [question], is there a market for it and what's viable from a business financial point of view. It takes five years to evaluate a product by the time you get it out. At the lower levels you're allowed to have a change control system and continue to update your system. At the higher levels the view was you weren't supposed to change it because it's the thing you verified and did this code spec on, right? So there was a lot of overlap and, as I say, it seemed — not to point fingers — but it really felt like it was more of the aerospace team here in California, teams in California, that were working on the C2, B1 areas, where the adversarial became quite difficult at times. I don't remember a lot of people at MITRE, though Rich Graubart at MITRE was doing database systems evaluations, and that's when we started seeing the TNI, and the other parts of the rainbow series that were being developed. It was an attempt to create more specialized criteria for specialized components so that we weren't always trying to interpret the Orange Book. Yes, that's when they stood up the interpretation forum on Dockmaster, which was fun, too. I mean, so there we were using a MULTICS computer system that was running at NSA and it had a forum for tracking the subject threads and conversation, and I think that's when that was set up. I think Dan Edwards really sort of weighed in when things got adversarial. He probably was hearing the most from the

companies and business people saying: essentially, your evaluators are costing us time and money, they're going crazy, they're nitpicking over a line in the TCSEC, how do we get past this? Then they set up the forum for discussion. Marv Schaefer moderated a lot for them, and tried to weigh in, and then we had these meetings with both Aerospace and MITRE evaluation team, interpretation meetings, and meetings about all of us and trying to find ways to do it more effectively. But there was still a lot of these young people right out of school who really felt it was their job to find *THE PROBLEM* and nail the vender because they didn't meet some stringent interpretation. So, looking back it feels to me there was a disconnect and a little bit misguided. SCOMP was different because like I said, we felt like we were all one team and pulling together. Maybe I wasn't as objective as I should've been, but our goal was to get that A1 for everybody, and the goal of these other teams was to prevent them from getting something.

Yost: So you mentioned that the paper that you gave in 1984, for an IEEE symposium, can you talk about the reception to that?

Benzel: Again, that's a career turning point in my life, getting involved in the IEEE Symposium on Security and Privacy, which at that time had 200 people and it had all the names of everybody working in this field. I started working at MITRE [and] I think I went in my very first year in 1982, and attended the conference, and got to hang out with Marv Schaefer, and Dick Kemmerer, and all these people. David Bell was there, I think. And then I wrote up this paper and when I delivered it, my footnote at the end of

delivering the paper was, 'and Chuck found a fatal flaw that we didn't find through any of this process.' I was very nervous and very young, but my memory would be that it was still well-received because again, you're in a small room of the believers who were trying to do this process and you had in that room, Boyer; Moore; Don Good, who wrote the Gypsy verification system; you had the people in there who had written these tools. And I really think at that time, the community view was well, it can happen but if we had really done it right, we would've found all of that stuff. There was no sense of oh, this doesn't work, or this isn't useful, or gee, we're finding all this stuff without going through it. It really was how can we meet our exalted goal?

Yost: And had you gone to any of the National Computer Security Conferences at that point, and can you compare and contrast those two events?

Benzel: Yes, I went to all the National Computer Security Conferences and I've gone to — still — just about every IEEE Symposium on Security and Privacy since 1982. I missed two years when I was a vice president in Network Associates and it seemed very disconnected to what I was doing. National Computer Security Conference, well, they're just totally different, right? IEEE is a top research conference, it's a publication, it continues to be the way people get tenure, it's very much an academic environment. National Computer Security Conference is not really a publication, doesn't really count academically as a publication. And, again, I think it's part of that culture, with disseminating information to the community, clearly, but sort of an inward-looking kind

of love fest, if you will. I have a couple of papers at NCSC, too. It was a good place to get together and talk to people, and it was a good place for venders to come and get a good feel for what's going on.

Yost: In 1985, you began leading a project for MITRE [that] NSA-funded for investigating research in requirements for software verification environments. Is that something you can discuss?

Benzel: Sure. Again, I'm still a pretty deep believer and you know, the question coming out of the SCOMP evaluation for me was how can we build better environments and how can we begin to understand a mapping between the specifications that are developed on a DoD acquisition. So we have all these MIL standard specifications, right? And how do we create a verification environment because again, my belief is if we only did it right, we'd catch everything. So it was an NSA-funded project to look at what are the requirements for building systems from scratch with the formal verification methods as part of that. So a specific merging of software design engineering with software verification engineering.

Yost: I believe it was 1987 that John McLean gave a paper at the IEEE Symposium on System Z that strongly critiqued the underlying foundations of the Bell-LaPadula Security Model. What was your reaction to it and what was your sense of the community reaction to it?

*Revised to correct MIL, p.26.

Benzel: Yes, McLean gave a couple of papers in those years. System Z was really eye-opening for a lot of people. There were a couple of pretty strong papers that started to create the cracks in the emperor's clothes at that point. We had to start looking. I was pretty easily influenced so I think I kind of jumped ship and started subscribing to the things that McLean was saying but there were mixed feelings in the room. Actually, in these conferences around that time, there started to be some anger and real schisms in the room. There were people that felt it was an unfair paper and that in any of these places, because we're looking at a lot of complexity and a lot of subtlety; again, as a mathematician, you can prove anything you want to prove, right? So there were some in the community that were more aligned with the Computer Security Center and the Orange Book, who felt that this was an unwarranted attack and was just trying to prove a point to prove a point; and didn't really, you know, take us as far. I would say that the Rushby papers on non-interference that came out around that same time, or a year or two later, were more important in changing some belief systems. So maybe it had to do somewhat with the personalities and the way the papers were presented. I think that there were some really foundational papers, starting with System Z, Rushby on non-interference, some papers around on downgrade, some work done by Teresa Lunt on the SeaView database project. All of those really started to change some opinions, and that was the late 1980s.

Yost: When did the evaluation on VAX SVS come in?

Benzel: I don't know if I know.

Yost: Were you involved on it from the start?

Benzel: No, I was not. I was not one of the key players, excepting for Steve Lipner trying to hire me to come and do the verification part as a DEC employee. I had a number of colleagues that were working on it; again, primarily at Aerospace; Sue Landauer at Aerospace, I think, ran most of that; and then Kim at MITRE was working part of that. I think maybe Rich Graubart was part of it. So it was one that was discussed a lot, and then I spent some time considering a job offer from Steve Lipner. My daughter was born in 1985 and I think she was one or two years old when I thought about that; maybe 1986, 1987; I don't know.

Yost: Would you characterize the relationship between computer security researchers at MITRE and Aerospace as more cooperative or competitive?

Benzel: Competitive, very competitive, right? Very competitive and very opinionated. I became very good friends with some of the evaluators at Aerospace, particularly Deborah Downs, who ran that group there. And I was one of the few that spanned teams because those of us that did verification were a pretty small group, so we really spanned. I flew here to California frequently and was on the Gemini evaluation team, bringing my

knowledge from SCOMP, but Gemini was led by this group here, out of Aerospace. I think Deborah was actually doing them, not just managing the group. I think she and I spent a lot of time doing that; and of course, Cynthia Irvine was at Gemini at that point. But yes, we were really competitive and very opinionated. And of course, we at MITRE thought we knew better and that the Aerospace people didn't know what they were doing. And I still believe that the Aerospace people were more adversarial than the MITRE people because the MITRE people that we had, remember we had Grace Nibaldi, we had Pete Tasker, we had the people that had written the TCSEC. That was part of our history and who we were culturally, and so we were all pulling together to make it happen. Whereas Aerospace, still culturally today, their job is to be the one that looks for the problems in a government contracting kind of situation. They're the overseers of the problems and so that's their culture. We had different cultures.

Yost: Also in the mid-1980s, the field of intrusion detection research began to take off, the IDES project at SRI, and some projects at National Labs, was there a sense among people that were more on the high assurance side that that research shouldn't be necessary because a completely trusted high assurance A1 system prevents intrusion?

Benzel: [Laughs.] I think it was a very interesting time of shift. You went through this period of seven, eight years — maybe close to 10 years — in search of the holy grail of MLS system, and really believing that. And then all of a sudden, you move to well, intrusions will happen so how do I detect intrusions? And it's also around the time when

you start seeing the beginning of firewall technology, and we'll touch on that, which is [that] intrusions happen, how do I keep them out kind of thing. It wasn't so much that that, at least in my experience, shouldn't happen, but it was kind of a compartmentalization. So then it became much clearer that evaluated systems and MLS systems were this small niche market inside classified systems and we were really focused on MLS. And MLS didn't translate to industry, and industry was starting to have attacks that went beyond simple virus signatures. So I think there really became a split, and I do believe the relevancy of the criteria and the Computer Security Center started to diminish.

Yost: What are your earliest recollections of the VAX SVS evaluation, and can you kind of take me through that from your perspective?

Benzel: I wasn't all that involved in it. I think the best I could say is it started out with some of the same idealism associated with it, like what we had with SCOMP. But the realities of DEC Corporation as opposed to this small government systems group at Honeywell, really started to intrude pretty quickly. And by then, also, the criteria creep that was happening, and the interpretation — increasingly rigorous interpretations made it harder and harder to meet that. And the verification tools; another thing that had happened was that this early first generation of verification tools that we had used for SCOMP had not kept up, in a sense. HDM was no longer a supported system so they had to use Gypsy, but Gypsy has a different model of operation than HDM. So in a sense, you

had an Orange Book that had codified an HDM-style Boyer-Moore Theorem Prover style there, and now you have the Gypsy verification environment which is a little bit different in how to do it. So the difficulty got much harder. It really started cracking pretty early on. I don't remember much of a honeymoon with SK VAX.

Yost: You mentioned DEC as a corporation. One thing in the paper by Lipner, Yaeger, and Zurko is they mentioned Conway's Law and the architecture of the system reflecting the organizational structure. Something [Conway's Law] journalist Tracy Kidder latched onto and popularized in *The Soul of a New Machine*. Is that something that you saw at all?

Benzel: [Laughing.] No, I don't think I could comment on that. I'm sure they have a much better view of that than anything I could add.

Yost: One of the conclusions in their paper, looking back, they wrote "fundamental to VAX SVS development process . . . results may be obsolete on delivery." Do you think that's a fair assessment?

Benzel: Absolutely. But see, I think, again, our perspective from SCOMP was it was developed with verification from the beginning. It grew out of this thing at the Naval Research Lab, and was adapted to the military message system. So it had a long history from its very beginning, to be built by a government systems group that was building a

formally verified MLS system. And I think SK VAX, and VAX, and DEC as a company, were not on the same page. And I think we saw some of that, too, when we started to work at the B1, B2 level with IBM and Amdahl. They were trying to put on additional stuff that was being added onto a system that wasn't built with high assurance intended. Now you can also compare and contrast that to the Gemini system, Roger Schell's system. Roger's was built with verification high assurance from day one. Today, still, in 2014, Roger will talk to you about high assurance and the Gemini operating system. That one, in a sense, stands in time and history as something that's a high assurance operating system.

Yost: What was your view of the lower levels, in TCSEC and the commercial products that had come out in the mid to late 1970s, RACF and ACF2?

Benzel: I had a lot of interest in them again, just to try and prove out concepts in the Orange Book as we're moving from the Green Book to the Orange Book, from the Nibaldi to the Orange Book and through the Tasker edition. At the time I wasn't very interested because I was really single-mindedly on verification and operating systems. Security — it's kind of hard to say this — but in some way, I wasn't all that interested really in what the security was that was achieved by this effort. It was more for me about the journey than the destination, if you will.

Yost: So the mathematics and the logic.

Benzel: Right.

Yost: Were you disappointed when the VAX project was shut down for business, financial reasons?

Benzel: Yes, it was really sad for all of us. I was definitely disappointed. It was a really hard decision and I know some of my colleagues who were doing that evaluation really took it very hard and somewhat personally. Again, those that are sort of on that inner circle believed what they believed and didn't want to think about those realities that were out there, and felt it was short-sighted and if DEC really only understood. But I can't really characterize what that experience was like though, and understood very well what the decision points were.

Yost: So you have these academic papers by Rushby and McLean, on the one hand, providing critiques. Can you characterize the impact beyond this, of DEC not going forward with marketing that as a deployed system?

Benzel: Yes, DEC's decision certainly had ramifications even down to the lower levels. There were many companies that were involved in evaluation at that point, who were very concerned about the amount of time it took, and the currency of thing that got evaluated versus the thing that they were selling. At the same time, I think the Computer

Security Center was rapidly turning out the rainbow series, sort of in a reactive mode. If we can make the component small enough and tailored enough in a particular way, we can still have some relevancy here. The other thing that happened at the same time is the internet. So I mean, SCOMP, now that I look back on it, sure, it was easy to be secure, it wasn't connected to anything, right? [Laughs.] But when we started connecting all this stuff up together, really, the whole evaluation criteria just fell apart. It just falls apart when you got there. And we must be coming up around the time I left MITRE, and left evaluations, and moved to TIS, because I don't think after that I myself had much to do. How are we doing on time?

Yost: Just over an hour.

Benzel: Okay.

Yost: Obviously, some internal analysis, economic analysis went on with both the project team, as well as with others within DEC. To your knowledge, were very many people looking at and riding on the economics of computer security? I searched and I didn't find much literature.

Benzel: No, I didn't hear anybody bring that up at all; anywhere in the 1980s and well into the 1990s, even, because all that stuff was built by the NSA, the Orange Book, and all that evaluation process; and I mean, the NSA was paying all of us through MITRE

and Aerospace to do the evaluation and industry was putting all this money into it. That was all billed in the quest of multilevel security and that's not an economic issue. Inside the DoD or inside the NSA, this is not about economics this is about protecting the nation. It's when you bled down into the C2, C1 and the RACFs and ACF2 stuff, where you're trying to put some level of security into industry commercial products that those questions have to come into play.

Yost: Can you tell me about your decision to leave MITRE and join Trusted Information Systems as a principal computer scientist in 1988?

Benzel: It's a mixture of I'd been there for seven years, the evaluations were changing, I'd picked up these other projects for the National Computer Security Center, I'd sort of moved my interest more into software engineering and software development and how you can have increased assurance, if not high assurance, in those areas. There were some personality changes, some management changes. I was a group leader. [I] wanted a promotion I didn't get it; someone else got the promotion. I wasn't as comfortable with the structure of that organization at that time. And at the same time, I had a two-year-old daughter. My in-laws lived in Connecticut and gave me that family support that I needed but my family's always been in California, and my husband lost his job. There you are in the middle of the winter, it's January in Boston, and you're schlepping the kid to daycare, and you don't have any family support, and my husband didn't have a job. It was time to come home to California.

Yost: And so from the start at TIS, you were in Los Angeles.

Benzel: Yes, I've always been in California since I joined TIS. I came here and I interviewed with Steve Crocker, who ran the office here in Los Angeles, and then I interviewed also with Rich Feiertag, in Menlo Park, who ran an office of I believe the company's called ORA, Odyssey Research Associates, and their headquarters were in New York. I interviewed with both of those, and we decided on LA and Trusted Information Systems. So there was a small office here when I joined it. When I joined it, I might've been number six of seven; we were under a dozen people when I joined it.

Yost: Do you have a rough idea of how many employees were at TIS in the 1980s?

Benzel: I think I was employee number 40, because I think I remember my badge and I was right around that number.

Yost: Had you had a chance to get to know Steve Walker, prior to joining?

Benzel: No, when I joined, as part of my interview process I did interview in the Maryland office as well as here. But when I joined, I think the only person I really knew was Sue Landauer, who was here in the Los Angeles office, and had been on those A1 evaluations with me, so I had worked with her on some of those evaluations. I think that

was my point of contact. I didn't know those people at that time, but it was a small company and I quickly got to know everybody.

Yost: Can you compare and contrast the culture of computer security research and development and consulting for MITRE and TIS?

Benzel: I'm going to close those blinds because it's getting a little too warm. I love my ocean view, but in the afternoon it does get warm in here.

Benzel: Okay, so your question was compare and contrast the culture of computer security research and development at MITRE versus Trusted Information Systems. Oh, big difference. MITRE is a federally funded research and development center, captive of basically the Air Force and NSA. The group we were in was primarily supporting the National Security Agency, and we didn't have to write proposals to be funded, because we're a line item in the federal budget. There were certainly politics that happened inside MITRE, but at my level, the money was just there and the projects were just there. You go to Trusted Information Systems, it really had an entrepreneurial aspect to it. I wouldn't say startup at that point in time, but it was very entrepreneurial and we all had to write proposals to get our grant money in. But we also had this feeling that we were on the inside, because Steve Walker, after all, had helped found the National Computer Security Center and that whole level of work that was there. And then DARPA, we had very, very good relationships with people at DARPA, and most of our work came out of DARPA at

that point. We weren't supporting evaluations as much as we were supporting DARPA and doing research. I think my first research project at TIS was one for Rome Labs, for the Air Force; again carrying through my notion of software development and specification, and software engineering so I started working with Rome Labs in that area. This office here was very small and very entrepreneurial, at that point.

Yost: At that point in time with TIS, was there much consulting business outside the defense and intelligence communities?

Benzel: Not early on, from what I remember. Later years we certainly did a lot of consulting with the companies. I guess my first few years with Trusted Information System was possibly before SK VAX was cancelled and Sue was still supporting that, but I didn't do much evaluation work when I got to TIS. And at that point, we're working on fairly large, mostly DARPA contracts, and a couple like with the Air Force, and Rome Labs, and I think maybe some with the Navy. Steve Crocker was still doing verification; so Steve Crocker, Hilarie Orman, Sue Landauer, Tim Redmond, and there was a bunch of papers in those first few years when I was at Trusted Information Systems because they had a verification system, but they were trying to do hardware verification. So it had a different context, and it wasn't in the context of an Orange Book kind of evaluation. I think it was being funded out of the Navy to do hardware level verification.

Yost: And from your CV, there's four projects that you list. Could we go through those?

Benzel: Sure.

Yost: One is lead engineer for a consulting effort to Hughes Aircraft on information security on the Air Force F-22 project.

Benzel: Yes, that was a lot of fun. I wasn't quite sure of the chronology of when I started work on that. The F-22 had a requirement for a multilevel secure computer. It's not the thing that flies the plane, but it's a data processing system that's in the F-22. Hughes had hired our Trusted Information System group here in Los Angeles. Mary Bernstein worked with me on that. We had offices down at Hughes and brought a lot of knowledge and background from the Orange Book; and there was an NSA certification board, but not evaluation, it wasn't being evaluated, but it was part of a DoD acquisition. Really what the work we did for them was in architecture and design, and specification review. I'd have to say again, one of the high points of my career is a paper I wrote with Marv Schaefer, but I don't believe it was ever published, because the F-22 used a 33-bit tagged architecture on [an] Intel 80960. Maybe I published that at NCSC. It was very, very fun and very interesting because now you felt like you were actually making a difference because you were actually building an airplane. If you go back, my master's thesis was on the F-15 so here I am again on a new fighter aircraft. And again, a small, elite group inside Hughes. Building an F-22 you can get completely overwhelmed with processes, and government, and blahblahblahblahblah. But there was this small, elite target team

inside Hughes that worked closely with us. So first, architecture and design, then support for the certification — not really verification, but certification analysis of it — and specification and design review.

Yost: And the next entry, researcher on a DoD-sponsored effort for integrating security requirements with DoD standard 2167.

Benzel: That was fun. That's the one that was actually out of Rome Labs. Emily Swiekarawicz was program manager, and John Faust, at Rome Labs, and had kind of grown out of the last work I had done at the MITRE Corporation. Again, really believing that if we did the right thing from a software engineering point of view, and from the beginning, we could get to that level of security so when the DoD acquire the system they had these military standards that you have to go through. So my project was to integrate them with some of the formalisms.

Yost: PI for an Air Force-sponsored integrated trusted system development environment.

Benzel: That's the next one I did; I guess this is somewhat chronology. Once you agree that you understand that you need to make a specification process and a development process, what are the next steps that you do in building a trusted software development environment? To do that, and what are the tools that you want to bring together to do

that. Mary Bernstein, again, and John Sebes were my collaborators on that effort. I don't remember that one going very far, but I'm not sure.

Yost: And then principal computer scientist on a DARPA effort on a trusted real-time Mach operating system.

Benzel: What we did was we took the work that we had done that was specific to the F-22, and we went to DARPA and sold it to DARPA as a research project. Not a DoD development thing, but a research project. And there the real study was a trade off between how you could do real-time computing and embedded computing, and be trusted. There was specialist hardware that was involved in it, and I really started branching out because I came out of an operating systems and math background, and now I'm looking at hardware specifications for the Intel 80960. Marv Schaefer helped me a lot with that project. That was a really good project. I think that kind of work continues to be seen in influencing all the cybersecurity emphasis on embedded systems and SCADA system, and I think that was the beginning of people thinking about those issues. Prior to that, most people thought that real-time and computer security were orthogonal and couldn't come together, because there really was this common belief [that] you pay a penalty for doing computer security. Not that me or we proved anything that no one else had started working on, but the community started thinking about that, forced by things like an F-22 fighter really needs to operate real-time so how do we do this? [Laughs.]

Yost: After you joined Trusted Information Systems, you become director of the Los Angeles office, the West coast operations of the company. There were roughly 50 research staff at that time. Obviously, your career had taken a much more managerial track. Can you talk about that and talk about your management philosophy?

Benzel: Right. So Steve Crocker had left Los Angeles and moved to join TIS in Maryland. Family took him back to the East coast again. So we were left with a little bit of a management void. We spent a painful year with myself, Sue Landauer, and Hilarie Orman as a troika trying to manage the office. In the end, that wasn't very productive; and in fact, Hilarie left to join the University of Arizona, and Sue moved to the Bay Area. So then it was clear. I have to say that throughout my career — it doesn't always come out in our discussion — but throughout my whole career I always had a bit of schizophrenia about whether I am a deep researcher, coming out of my family of Ph.D. academics, or am I in management? I had been a group leader at MITRE and left that; became an individual contributor; and then this is a time when it became clear to me I wanted to be in a position to manage people. I enjoy, and have continued all these years to enjoy the people part. Also, I have a real joy and hunger for going after the money. I like working with people and helping them write their proposals and target their efforts to go get the money. It was a challenging time because the majority of the company, the heart of the company, was in Maryland and we often felt like the stepchild. I got militant about that at times, and really worked very hard to not just manage us as a separate organization, but to be a part of the main organization.

Yost: And obviously, you're interacting with Steve Walker on a regular basis.

Benzel: Yes. I participated in senior management meetings with Steve Walker, Martha Branstad; all of the leadership of the company had weekly senior management meetings that I participated in over the phone. That year or the year after, there were a couple of years there where I flew over 100,000 actual miles in seats, LA to Baltimore.

Yost: Can you talk about Steve Walker as a leader?

Benzel: Yes. You know, Steve had a paternalistic aspect to his leadership. I don't mean to sound negative; I mean he really cared about the company and had a very humanistic aspect to him. He really cared about the people and taking care of all the people in his organization; and he had a real good sense for what's right and wrong, and he sometimes came up against different organizations in the DoD because he held really firm to what he believed in. He made regular trips out here to LA to meet with us and to spend time with the whole office, so that everybody saw him and had an opportunity to interact with him.

Yost: And Marty Branstad?

Benzel: [Laughs.] You know, Marty's one of those people that always raises the bar. I learned a lot from Marty because no matter what I did, I never felt like it was good

enough and Marty always had something more that she wanted from me. So she and Steve were kind of counterbalances to each other because Steve really, at the core, was a softy and really cared about the people, and didn't want to say the things that weren't popular or didn't make you like him. Marty, you know, was pretty hard core about everything and would take the hard decisions, and make the hard decisions, and tell you what you were doing wrong. I remember feeling pretty pained about that period in time, but when I look back now, I'm very grateful to Marty. She taught me so much about writing proposals, interacting with DARPA, interacting with customers, and managing people. Because she was the beginning of my management mentors that said sometimes you have to make the hard decision and make the unpopular decision.

Yost: Into the end of the 1990s, were opportunities emerging for doing business with industry as well?

Benzel: That's when really we'd moved as a world, as a community beyond just small MLS; the security is affecting everybody, viruses are rampant, systems are getting broken into. It's really the beginning of the age of cybersecurity. And I think that both Marty and Steve attracted industry that came to them and asked them for help because they were seen as such leaders in the community. And so with our industry connections, it was not a lot of pounding the pavement, it was really people knocking on the door and saying can you help us? We have a security problem, how can you help us? That was a very exciting phase for all of us because again we're making a difference. We helped Microsoft, we

helped Shell Oil, we helped corporations that were trying to build secure computers; what that meant. And then, when we started with the firewall and the firewall toolkit, and had the opportunity to start helping companies to install those firewalls and to architect their systems, and to provide that basis for it. It was a great time.

Yost: Were you at all involved in Trusted Xenix?

Benzel: Not much. I think that my involvement with Trusted Xenix was as a manager with people who worked for me. So Doug Rothnie was deeply involved with it; I think Sue had some relationship to it. It had some hard political ramps it had to overcome and so I got involved in that from a management point of view, but I don't think I was very involved from a technical point of view. But it was one of those ones where Steve kind of went out on limb, right? It was IBM that had built a Xenix, Trusted Xenix, and they were going to abandon it as companies were starting to abandon evaluations. Steve really still believed in the evaluations and we hadn't yet had a good case of a B2. We'd found a B1 and an A1, but we hadn't really had a good B2 yet. So Steve's view was that Trusted Xenix could be made to be B2. And so now, as an organization and for people like me, we flipped personalities because now we're not the evaluator trying to find the thing that's wrong with it, now we're the system developer trying to get through the hoops. And so you saw it from a different side. Unfortunately, it, too, was one of the ones that had difficulty passing its evaluation criteria.

Yost: Who were the primary competitors to Trusted Information Systems in the years . . .

Benzel: I don't think we had any competitors; I don't think we ever did.

Yost: . . . early on when you were leading the LA office?

Benzel: I think Trusted Information Systems is just unique in and of itself. I don't think we ever felt that we really had competitors. There was this other small company that Rich Feiertag had up in the Bay Area that was originally started by Richard Platek in New York. But they closed and we bought the office I had interviewed with in the Bay Area; we ended up buying them and merging them in; or accepting them, or something. So it's a one-on-one competitor at that level, that went away. Sure, when we competed on large DARPA contract awards, BBN, SRI, those kinds of organizations were competitive; and academics. Trusted Information Systems going after large DARPA research contracts, and we're a funny kind of research organization at Trusted Information Systems and so sometimes we had to compete head-on-head with Columbia or Cornell, or U Penn, those kind of places. But we actually did a very good job at collaborating and joining teams. In fact, in competition with somebody the other day; we work with Jonathan Smith at U Penn while we were at TIS on a large DARPA program called Active Nets. So you can go back through all of those and I just don't see TIS as having any competitors, so it was a great place to work.

Yost: What was the mix of projects where the company just came up with the research proposal versus responding to Request For Proposals for a particular type of contract?

Benzel: Early on — and it was also more a function of who DARPA was early on — it was ideas. And again, a learning experience for me, Marty Branstad took me into DARPA to brief an idea I had to Brian Boesch, [and] Steve Squires. At that time, it really was those people, Marty and Steve had the inside, they could call those guys up at DARPA, they would take us in, we could brief an idea and get a contract. As later years went on, it's more a function of who DARPA was and how they changed, how they were doing business. And as the directors changed, then it became more BAA [Broad Agency Announcement] responses. But also as a company, we were very, very diversified — probably more than anywhere I've ever worked — in terms of funding sources. So it wasn't all DARPA and it wasn't make or break it with DARPA. Like I said I did a lot of work with the Air Force Research Lab. We had the places like the F-22 in Hughes. We had Microsoft and Shell, and system companies, IBM came directly to us. It was a really nice diversified mix.

Yost: That's something to really push your leadership.

Benzel: Yes. In my leadership, I really pushed that we should always look for new opportunities. And I think TIS really exemplified what I call today, relationship-based marketing. So it was really a lot about who you knew, than a DoD acquisition

competitive award and so I really worked on my management style to make sure that everybody who worked for me had an opportunity to meet with the funding agencies, to meet with collaborators who might have been competitors. Again, it comes back to I think a lot of things in my management style and what I care about, is organizational behavior. Later on, when I did an executive MBA, that's one of the things that's important to me; how does an organization behave and how does it behave towards its people, and how do we work with our customers, because we're all one.

Yost: I know that in the services contracting realm that Computer Sciences Corporation became very effective at obtaining government contracts. Did they move into the computer security space at all in the 1990s or did that come later?

Benzel: I started seeing that. I think we actually ended up teaming with them a few times. So that became a little bit of a tension in the company, which is [the question] are we a services organization or are we a research organization? Where are we on the spectrum of services, research, research and development? In that spectrum. We took many, many different cuts at doing that, creating and carving out a separate services organization. I think Curt Barker might've run that for a while for us. These are our consulting people, these are our DARPA researchers, and these are our system builder people. But I think that Marty understood the value in more of a blended approach, and I certainly believe that still today. I think we're better researchers if we see the real problems that happen in the real world. And so many, many companies, especially in that

timeframe, [had that] as a business paradigm. Today, most businesses know how to put themselves firmly in one of those others, but in the 1990s, in the whole computer and computer security, that paradigm was difficult. So TIS is much more than just a consulting services company since we never wanted to be just a services company.

Yost: In 1998, TIS is acquired by Network Associates. Can you tell me the context around that?

Benzel: You skipped 1996, [which] was our IPO. So let's start with the 1996 era, which was the IPO.

Yost: Definitely.

Benzel: So we'd done the Trusted Xenix, which we thought maybe was going to make us money, it was going to be a product — it wasn't — so then we stumbled upon the firewall, so I have to tell you the firewall story. It's not necessarily my story, it's the story of Trusted Information Systems. I wasn't directly involved, I was off doing my little research thing. But, when President Clinton took office, he said I want to get on the internet. I want the White House on the internet. This internet is this new thing; I want to be on the internet. His Office of Science, Technology and Policy went to DARPA and said okay, you know something about this internet. Figure out how we do this, and we do it in a secure way. DARPA called up Steve Walker and said Steve, figure this out. So the

group there in Maryland with Marcus Ranum, who joined us from DEC at that time, and Fred Avolio invented a firewall toolkit under DARPA contracting. The firewall toolkit was installed at the White House. I was trying to remember another name that came up but I just blanked on it. So we installed it at the White House — no, first before we put it in the White House, we ran it at TIS in rural Maryland. In those building out there in Maryland, ran this firewall toolkit, taking traffic from the White House being directed through us. Periodically, I understand — I was here in LA but from what I've heard and I've seen pictures — men in black suits with little wires in their ears showed up in rural Maryland and said, what is this? This is bad, and they all got through your firewall. What are we supposed to be doing here? We had these guys in a back room hacking away at it. Got shook out, got installed in the White House, so then Steve went to DARPA and said what do I do? Now that I have this firewall toolkit that we customized and built and put in the White House, what do we do with it? DARPA said you make it open source; that's what you do on a DARPA research contract. Why don't you post it somewhere and see if other people want it, because the one in the White House is customized, the toolkit customized and specialized. So we did that and that's when major corporations came to Trusted Information Systems and to Steve and said, we want this toolkit but we want it not as a free download off the internet, we want you to give us a supported, maintained, applied and patched product. So the first company I believe that came to us was Shell Oil, and they were a global international company that wanted to be able to use it in their global systems. Really, we didn't have a price list for that. I mean, we were still Steve Walker's company in the garage doing DARPA research. We had not yet hired our

commercial people, right? From what I've heard — I wasn't there in the meeting but from what I heard — Steve says, literally, we sat around this table in the conference room in Glenwood, Maryland, and kind of looked at each other like well, how much should we charge for it? How do we charge for it? And that was the beginning, too, of those conversations of is it a service or is it a product? Is it a turnkey product? Okay, we know how to do that. We'll charge a certain amount of money for this box, and we ship it to you and you plug it in, and now you have a firewall. Well that didn't work. Very quickly those companies said unh, we don't know how to install it. So now we need a consultant who flies around the country with the box and helps you install it. Then you back out and you really need a consultant to help you understand your architecture and how you're going to do it, and all that. So that was the beginning of the firewall project, which became the Gauntlet Project. So then there came a couple of years of trying to determine how to commercialize that and make money out of it. Steve did not want to go down the path of venture capitalists, he didn't want anybody else's money or ownership. It was his, it was his baby, he wanted to own it and control it and self fund it. I think somewhere there is when Steve Lipner came and joined us, and ran our product division, because Walker admitted he's not a product guy. Marty wasn't a product guy, right? So we had Steve Walker and Homayoon Tajali, and that whole group ran this product division with this firewall in it. Eventually, Steve agreed to have an initial public offering for it, so we had an IPO in 1996. We raised $40 million. Not a bad raising; it wasn't the peak of the upward cycle but we weren't yet into dot bust at all, so it was a good showing. There were different valuations that could've come out higher when we first started on the

process. During that time, I went and got my MBA, an Executive MBA at UCLA. So that was fascinating because I'm participating in management meetings when we're having these discussions about valuations and public offerings and all that, and then I'm going to night school and learning those things in a classroom. Sometimes they weren't the same and sometimes they were. And then I looked back and I must not have slept for a year because how did I participate in a company that was doing this, and do an MBA, and have two kids?! [Laughs.] After the IPO in 1996, we were bought by Network Associates in 1998. You know, 1996, 1997 things went sort of okay. We had some money; we had a commercial organization; we're doing all the marketing and commercial things you want to do; we opened an office in London. But it became obvious — and Steve will talk about this — but it became obvious that you really need to eat or be eaten. To maintain valuation on the stock market, especially at that particular time, you couldn't do that on a single product company and $40 million. You had to have earnings estimates to keep growing, and how do you grow? My understanding — and again, I'm one arm's length away here in LA running a research group that's doing research stuff — we didn't have product people here that were part of that organization; but my understanding was that we attempted to buy PGP Security, thinking that's a good acquisition for us, culturally it's the same, all those things. Well, we were outbid by Bill Larson at Network Associates. Once we were outbid and not able to make this acquisition that was going to help us with our earnings, then it became clear we needed to be bought. My understanding, again from a distance, is that Steve was able to make an arrangement with a company that I believe was based here in LA and had a relationship with Jerry Popek from UCLA for us to be

bought. It was a friendly takeover and everything was going well. Steve talks about this pretty openly, they were literally sitting in the conference room in Maryland getting ready to sign the papers for this friendly acquisition that had all been worked out with everybody, and Bill Larson at Network Associates, who had outbid us on PGP, swooped in with a counter offer to buy us which was significantly higher than the prearranged deal. And you have stockholder fiduciary responsibility, you have to accept that higher offer. So he accepted that offer. Culturally, the two companies and the personalities could not have been more different. Absolutely, it was a very, very painful time. Steve had built that building right outside of his house in rural Maryland; he provided lunch for everybody every day; he cared about everybody; retaining employees and employee happiness; these were things that were extremely important to Steve and like I said, a paternalistic view. He cared about each of us; he walked around at Christmas every year with bonuses; he kept the earnings from his company and turned them back to the people; he offered stock options to us even before there was such a thing as a stock option. I mean, we were one company and we believed. Bill Larson was a shark in Silicon Valley and cared nothing about people, and only cared about money. Super wealthy Silicon Valley, you know, the fancy sports car, the fancy clothes; Steve's just not that; he's just this home person. Larson came out to Maryland for the handing over of the company and ridiculed our baloney sandwiches, ridiculed the culture that was there openly and blatantly; attacked our lawyer in front of the whole company. It was just heartbreaking. Heartbreaking. I'll cry. You know Steve cried that day in front of all of us because he created this thing of beauty and — I mean, I had the Undersecretary of the DoD tell me

that Trusted Information Systems was a national treasure. A ***national*** treasure. He truly had created that and this guy came in and just decimated it. He didn't care. All he wanted, really, was our sales list. Our product and our sales list. He didn't even care about who the people were, he just wanted to take that product. He had a vision and his vision was he acquired 35 companies in 1998. And his vision was he was going to create the *uber* computer security platform all in one, everything you ever wanted for computer security. His vision was it was going to be in one box and he was going to sell it and it's going to solve everybody's problems. He was misguided and that didn't happen technically, but that was his plan. So he bought 35 companies and smushed people together, didn't care, had a Silicon Valley view, developers are developers, who cares? Throw them away, I'll hire a new one. Just wanted the intellectual property, I want the tax write-off on the intellectual property, and I want the intellectual property and I want your sales list. Who are you selling that to right now? So Steve, and Marty, Steve Lipner, all the people that were one level above me at Trusted Information Systems, they all walked off. Believe me, Steve walked off with lots and lots of money, but it didn't matter; he lost this beautiful thing. And as a person who had just finished my MBA, he lost this beautiful thing because of the stock market and capitalism. There was no reason that it had to do that, excepting that that's how you do earnings per share in today's society. So they all walked off. This company came in and bought us for the firewall product, for the sales list and IP, and a tax write-off. So they brought out — not Larson the next time — they brought out their CEO and they brought out their CFO, and met with this research group, which at that point in time we had 120 people, we were doing $19 million a year in

revenue. They didn't even really know that they had bought that, because they had just seen the other side of the company. So they came out to meet with just this research group; the group leaders, of which I was one, and I was the office director here, to meet with us in Maryland. The CEO and the CFO started peppering; each one of the group leaders was supposed to give a talk and I had rehearsed a number of people in my group who were going to give a talk on what my group does. We had the crypto group, and we had the intrusion detection group, and the database group. And they just start hammering on, you know, well what's your backlog? And what's your average burn rate? And all these financial questions. Because I had just done my MBA and it was something I had always been interested in — you know, I knew all those terms and I'm kind of Marty's right-hand man; she ran the research group — on understanding, I mean, I spent a lot of time with Marty because I had to do the financial coverage assessment for all of LA, I often worked with her over the total financial assessment picture for all of us. I love the spreadsheets and loved getting into that. I'll never forget, one of my colleagues who ran one of the other groups, leaned over to me partway through the conversation and said [in a whisper], Terry, what are my numbers? He didn't know how to speak that language. I knew how to speak that language, right? So in the end, they offered me the job of vice president, of bringing that 120-person lab into the Network Associates culture, with their expectation that we would do technology transfer. DARPA pays for the research, we're going to grab it and make products out of it. I've been around tech transfer for a long time, it doesn't work like that. There's this huge gap; Doug Maughan calls it the valley of death. You build stuff under DARPA, there are research prototypes, you've got a product

here, they're not the same. We tried. We really tried, and we did spin off a few things in what ended up being the McAfee product line and some successes. But it was okay, because at that point in 1998, the company was flying high. You're in Silicon Valley. We're almost a billion dollar company, 35 companies merged into one, great big huge visions. They sort of didn't care because when you run a research group funded by government contracts, you completely break even. You can charge back to your government contract your rent, your telephone, everything; you're completely break even and you might make under 10 percent; five, six, seven percent that you can reinvest in more research. I pitched that to them and they all agreed. I really feel like at that time, I was like their little dancing doll on a charm. So I would go out with the top salespeople and go to Walmart, and State Farm, and CitiBank, and they'd say, 'you're going to buy our product line; we're giving you the super *uber* computer security box that you need. And the reason you should buy it too, is because oh, we have this research group. Terry, stand up and say research.' And I'd stand up and say we're looking towards the future for you. Our product will be even better because we have this research group. That worked for a few years. Then it was Christmas, December 27, 2000, and the board of directors fired the president, the CEO, the CFO of the company because they were being investigated for stock manipulation. So I got a phone call from a vice president, we're leaderless. The board fired everybody; there's nobody left but you guys as vice presidents. We've got a nationwide search going on. This is what's happening. Pull your troops together and do what you're going to do. So they pulled in somebody from IBM who'd been global sales manager worldwide for IBM as the turnaround came to turn the

company around. He did a good job of turning the company around and was receptive to the research group even though we hadn't proven that we were going to make money for them. He understood the break even and he'd been at IBM, and he knew what Watson Research Lab was, so he was supportive, again keeping us in that role, pushing on tech transfer type of thing. Well, so that lasted really 2001-2002 timeframe, and they got our stock price back up and things were okay. And then the SEC investigators came back again with another investigation and another damning piece of evidence. Not really pointed at him, but it was enough so that it was still on his books, and the stock crashed again. He couldn't tolerate keeping a research group any longer. He came to me and said we're evaluating people on earnings per head, not earnings per share. Earnings per head. What do you look like? Five percent, maybe, versus McAfee shrink wrapped software. We're not in the same book, right? So in 2002 we made a decision to divest ourselves and slim down, because we were still at about 120 people and still doing it. At that point, they all reported to me with a set of group leaders below me, again still doing about $20 million. I think when they acquired us we might have been at $17 or $18 million a year in revenue, and it went up to $22 million. So then we decided to divest the areas that were least related to the product line of Network Associates MacAfee, so then I had the pleasure of going to people who worked for me for 15 years and say, 'you're being sold. [Laughs.] It's really a good thing; we're going to sell you.' And got my MBA again; I got to learn about acquisitions and I got to learn about divestiture. And we did, we sold off two large groups and we slimmed down. I think we slimmed down to about 50 or 60 people. You know by the time we finished that in late 2002, and they were very focused

on having all of those people in Rockville, Maryland, which was close to a development team and the firewall people and that stuff, so there wasn't much left for me to do and that's when I made the decision to leave Network Associates MacAfee. It's a long answer to the question you asked. I don't think it's the question you asked but it's a story I have to tell.

Yost: A very interesting and important story. So when you said divest different research groups, who did —

Benzel: Yes, we took one group that was run by Russ Mundy, and we sold that group to the company at that time called Sparta, which was sort of a beltway bandit but largely did work for the National Security Agency. There was a good connection there, and it might've been 20 people or so. We sold them; I mean, we negotiated a price and sold them. The other group was by Sue Landauer, and she'd been working on some DARPA stuff, and one of the DARPA program managers had gone and created his own small company, and we sold them to that company. I'm afraid I can't quite remember the name because it was a real small privately held company. That one didn't last very long and they sort of scattered to the wind. Once that happened, even the remaining people in the organization I was still running started dispersing. That's a sad thing. You know, it was a national treasure and by 2003, it had just scattered to the winds. We still all connect with each other in various ways, and I still work with several of those people [pause].

Yost: Really an amazing team that came together.

Benzel: Yes it was. It was.

Yost: Trusted Information Systems, when I first started learning about the company, all these names, David Bell —

Benzel: David Bell, right; Steve Lipner, Steve Crocker, Steve Walker, Marty Branstad, Denny Branstad, it was just amazing, the people.

Yost: In 2000, you were appointed to the security panel of the president's committee of advisors on science and technology, and went to the White House several times. Can you talk about that?

Benzel: Yes. So now I'm at Network Associates; critical infrastructure protection becomes the buzzword. It started being a buzzword in 2000. Certainly by 9/11 it was the hot, hot, hot word, right? But critical infrastructure became . . . are we doing okay?

Yost: Yes.

Benzel: Became the buzzword so the president's PCAST [President's Council of Advisors on Science and Technology] stood up a special panel on critical infrastructure protection. So I was not a member of PCAST, I was a member of the PCAST panel on CIP. I had an opportunity to spend quite a bit of time in Washington, at that time, largely with large companies, many of them in things like transportation, banking, the different critical infrastructures of the nation. Now we really are into economy, we're really into the concern about the safety of the nation, not just of our military assets. And so that was an excellent opportunity, and fit with my role as a vice president at a major software security company. So they were very supportive of it and really liked to see that. I came across a picture recently of my first trip to the White House. Now I've been several times; I actually went twice this year, so it's still exciting. [Laughs.] But we defined that committee, PCIS, the President's Committee on Infrastructure Security, defined a number of standards and requirements. That whole area is a tough area because it's privately owned and operated so the government can't mandate legislation, but we tried to work cooperatively.

Yost: You also have testified before Congress?

Benzel: Yes, I testified before Congress the first time right after 9/11. I think it might've been a month or two after 9/11; pretty close in there, in October I think. And since this past year, 2013 I think it was, I testified again. The point is the discussion at the congressional level that's still an important discussion is how much do we invest in

research, in pure research versus product development and can we close the gap in the security problems that we face by putting more investment in product and services? And, of course, conservative Congress or conservative administrations believe the answer is industry has lots of money. Look at the Ciscos and all those companies. They have lots of money, why don't they put their money in and just build us more secure products, and then we don't have a problem. Right? Certainly not my view, being part of a leading university and having been in research all the way since NASA Ames when I was like 18 years old, right? And being on a more liberal political leaning, [the answer is] no, it's extremely important to do fundamental research in whatever way you can do that. And so those have been the points where I have testified before Congress, in hearings on bills that are authorizing large investments in research.

Yost: Within that time frame, the NSF is beginning to become a significant player in funding computer security research?

Benzel: Right. Well, it actually was my first testimony in 2001 as part of a panel of researchers [that] led to the authorization funding of the Computer Security Research and Development Bill, which gave NSF the significant funding that started their trusted computing program run by Carl Landwehr. Again, all the names keep coming back; we're still a small enough community over those years. Now, I'm going to have to say, when I testified before Congress to say Congress should create a funding vehicle, as such,

that does not mean that you're authorizing a spending bill; and I had the pleasure of testifying with many leading luminaries that also argued that case.

Yost: So you joined USC and ISI in September of 2003?

Benzel: Yes.

Yost: Can you tell me about the history of the DETER test bed?

Benzel: Yes. So there's a little gap in there. I left Network Associates in April of 2003 and I joined here in September 2003. One might've thought I was on the beach or vacating or something after all of that. But I didn't. You know the way things work. So Shankar Sastry was the head of the computer Science Department at UC Berkeley. He'd previously been a DARPA program manager. In our last year at Network Associates we wrote a report for Doug Maughan, who was at DARPA at that time, called Requirements for Distributive Denial of Service Security Test Bed. I have to go back a little bit. In 2000, the first large denial of service attack happened. It took down banks, ATMs, Victoria's Secret online shopping, right? My group at Network Associates came up with a solution of how they thought they could prevent or detect denial of service, or throttle it in some way. But we had no way of testing it at large scale. We could test it in our offices but that was about it. So Doug had funded us. He said write this report; what would you need to test it? So we wrote this requirements document. Doug then launched on an issue

of trying to get that effort funded to build the test bed. It had a $20 million price tag on our report. He spent all his time in Washington, finding somebody that would fund it. NSF finally said well we'll take a crack at some of it, and they had a study group, and put in a bunch of stuff like that. So now, NSF's going to be the lead on funding the building of a security test bed. I left Network Associates. Network Associates can't respond to it because NSF funds universities, not companies. You can be a sub somewhere, but really, funding has to go to a university. So I was in a meeting, like two weeks before I left Network Associates, with Doug Maughan and Shankar Sastry, and they said that's the answer: Terry, you go to Berkeley and we'll write a proposal for this NSF solicitation for a security test bed. So I left Network Associates on Friday, and I started at Berkeley on Monday and I worked with the UC Berkeley team to write the proposal for DETER. I commuted from here, I lived here, I had kids in school, but I lived at Berkeley every week, spent two or three days a week there, and worked with a really good team put together by Shankar to write that proposal. While we were writing that proposal, it became evident that we needed someone who would operate and actually build this test bed, and that it wasn't the Berkeley top professors, but somebody else needed to do it. I knew people here at ISI, so I called ISI and said well, Bob Braden and Cliff Neuman, you've run test beds before for the government and for DARPA, you want to join this proposal? They joined the proposal; we all wrote the proposal. The proposal did go through a full evaluation at NSF, a panel evaluation, and was selected for award at the end of that. The award date is September 2003. At the end of that summer, both UC Berkeley and ISI offered me jobs. I was just doing a consulting position at Berkeley,

trying to bring this in. I live in LA, I made the choice to stay here, and so I joined here, still actually being paid by; I don't know, it was a weird situation where we were subcontracting to Berkeley, and then eventually we moved the contract here and now Berkeley subcontracts to us on the DETER project. I don't think I quite answered your question, but that's the history of how the DETER project came to be. We've now been here for 10 years, 11 years.

Yost: Can you talk about some of the applications of the project?

Benzel: Yes. DETER has been operational, like I said, for over 10 years. [It] has thousands of users that have used it. In the early 2003, 2004, researchers were primarily looking at issues related to worms. The Slammer worm came out in 2003. Vern Paxson on that team did very good work that's been published in Worm 04. Malware was sort of the early intention of it and the early intention was the test bed, a closed environment, you can come run live malware and do experiments with it. Over the years, the range of research that's being done by the users is much broader. It includes core internet things, internet routing, name services, those sorts of things that make the core of the internet. It includes very complex malware that you see now in botnets. And over the last probably three, four years we've branched out into cyber physical systems. So the last couple of years we've been working primarily with researchers in the power grid that are bringing in these new smart grids and specialized meters, and so DETER now federates with specialized labs and other places. I just had an advertisement from PNNL, who I've done

some work with, they run their own version of a DETER that's connected to these specialized meters so we can look at security in these convoluted, complex situations that mirror merging cyber and physical systems together. And then the other major focus has been in education. It's really hard to teach students hands-on cybersecurity. You know, how do you let them break something in your university network or the real network. So Jelena Mirkovic, who is part of the team here, got an NSF grant, and I think we're up to now 26 different exercises that professors anywhere in the world can use to give hands-on experience in setting up a firewall, doing routing, doing these types of things. I call them turnkey exercises because we tell the faculty member [they] don't need to be an expert in the running of DETER. We say here's the exercise, here's the scope of it — one student, five students, weeks, whatever — here is a grading sheet, and we provide them the infrastructure to do that. I think we're up to 183 institutions have used it. I can tell you the students that get that experience come back to us, and they say that they're getting two and three job offers at top places because when they're asked in an interview, what do you know about firewalls? They're not trying to remember a multiple choice question or a chapter in a book; they did it and they know it. So it's been very exciting.

Yost: That's great. Is the DARPA-funded SAFER lab connected or is that something separate?

Benzel: It's separate. So the DETER test bed is actually funded now solely by the Department of Homeland Security; Doug Maughan at DHS. It's had NSF funding and

some DARPA funding over the years but it's been DHS for a number of years. DARPA has a program called SAFER to look at anonymity on the internet, and when they created that program one of the components of the program was to have an assessment vehicle; a place where all of the five teams that they awarded contracts to could come and run their prototype software and an independent team could evaluate it. We're not the independent team; there's a Red Team, if you will, that evaluates that. What we provide is what I call a level playing field. So all five different performers can come in and use the test bed and we get real apples to apples comparison. And then our team helps look at the integration across those, meta issues, while the Red Team is attacking at the level they attack at. And we also do performance, and archiving, and analysis of it.

Yost: In 2005, you became the Deputy Director for the Computer Networks Division. What new responsibilities did that bring and what are some things you worked on?

Benzel: When I started at ISI, I actually worked directly for Herb Schorr, our executive director of the institute. I focused on multi-disciplinary, multi-divisional research problems, and infusing cybersecurity in a lot of different areas here at the institute. At the time there was a networks division here that was run by Joe Bannister. In 2005, Joe Bannister left ISI and the institute hired John Wroclawski from M.I.T. to come and run the networks division, and asked me to join as John's deputy. So since 2005, John and I have run this division. We have 40 to 50 people, depending on how you count the number of grad students we have. I'm doing work in networking and cybersecurity. The DETER

project is a large project and a lot of people in the division work on it, as well as SAFER, when you put those together, but there are other groups that are doing their own research. And we have grad students. So again, I'm at that place where I have two hats. As a deputy director; roughly speaking, John and I split things where I'm the COO and he's the CEO, if you will, of our organization. He's very vision oriented, very outward looking, and I do a lot of the operations. Again, I go back to those spreadsheets, and our funding, and our coverage. I have a good financial analyst I work with. I do a lot of people, personality [work]. I've got the open door, they always come in and talk to me. But I run the DETER project, which is a very large research project of its own.

Yost: Before we conclude, are there any topics that I haven't brought up that you'd like to discuss?

Benzel: I'm running out of steam. I think you've done a really great job of your research and the set of questions you've asked. I'm glad I had the opportunity to talk about Trusted Information Systems in the way I could; it's really special. I think we've covered it.

Yost: Well, thank you so much. This has been extremely useful.