An Interview with

REBECCA G. BACE

OH 410

Conducted by Jeffrey R. Yost

on

31 July 2012

Computer Security History Project

University of Maryland, Baltimore

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

Rebecca G. Bace Interview

31 July 2012

Oral History 410

Abstract

Rebecca Bace, who has a Master of Engineering Science degree from Loyola College, is a leading figure in the computer security field of intrusion detection. She is the author the influential textbook on this topic, *Intrusion Detection*, and was leader of the pioneering Computer Misuse and Anomaly Detection (CMAD) Research Program at the National Security Agency from 1989 to 1995. In this capacity, she sponsored much of the first wave of path breaking academic research on intrusion detection. This interview briefly addresses Ms. Bace's education and early professional life before focusing on her dozen years at the NSA, and specifically her leadership of CMAD. In detailing the portfolio of early CMAD sponsored projects that Bace supported, it provides an important lens into the early evolution of intrusion detection as a research field and area of practice, and identifies many of this field's pioneering contributors. The interview also briefly touches on Bace's work after leaving the NSA, including at Los Alamos National Laboratory and as President of the consulting firm Infidel, Inc.

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 Charles Babbage Institute of the University of Minnesota, and I'm here today with Rebecca Bace at the University of Maryland Baltimore County Campus at the Tech Incubator. This oral history is sponsored by the National Science Foundation, CBI's NSF-funded project, *"Building an Infrastructure for Computer Security History."* Becky, I ran across that you grew up in Birmingham, Alabama. Were you born there, as well?

Bace: I was born in Birmingham. We moved when I was about the second grade, out to Leeds, Alabama, which is a wee bit more rural, about 20 miles east of Birmingham.

Yost: Can you discuss your evolving interest in elementary, middle school, and high school? Did you have any interest in electronics or give any thought to computers at that time?

Bace: Not too much to that brand of technology. I was raised by a very eclectic pair of parents. My father was a classic Sand Mountain-North Alabama redneck, who had an aptitude for dealing with engines. He went off to World War II and met my mother, who comes from a rather aristocratic family in Japan. My grandfather was principal of the Imperial Girls' School and my mother had a very luxurious upbringing until World War II hit. After Pearl Harbor, my father joined the forces and ended up posted in Japan. My mother went through a fair amount of the strife surrounding the shelling of Tokyo through World War II and the subsequent upheaval in the Japanese economy. Anyhow, they both came away with this with a vow that none of their children would grow up

incapable of being self-sufficient. So they used this as liberty to give us all a set of unusually well-rounded mechanical and electrical troubleshooting skills, to the limits of their capabilities. But also they had a fair amount of emphasis on giving us my mother's academic legacy; a fair amount of emphasis on doing well in school. Also, their focus was always somewhat quantitative. I have an older sister who's a mathematician; a younger sister who ended up in similarly analytic realms. But at that time and place, you kind of stumbled into the computing arena. I happened to hit school; hit college at a point where computing was just starting to become real in anything but the huge institutional settings.

Yost: I saw in an *IEEE Security and Privacy* article that you had an early interest in picking locks?

Bace: Not only in picking locks; actually, I had a serious interest—we joke about this now—I had a serious interest in what it took to assemble and optimize bombs, actually. (Laughs.) We cleared land; my folks moved us out to the woods; around Leeds, but into the middle of a significant piece of property and wanted us very much to farm. The only problem was we had a lot of trees. So the joke was my father realized that I was better at arithmetic and math than he was, so the first assigned quantitative task I remember having was that he would charge me with computing how much ammonium nitrate we could add to a particular portion of dynamite in order to service as an accelerant. But also, because of that—thanks to that—I know a little bit more about dealing with dynamite and explosives and was totally fascinated by it. The irony, of course, is that

ultimately, 25 years hence, it served as one of the door openers to one of the more pleasant collaborations of my adult life, with a fellow who was a principal in the arson and bomb section at Quantico, for the National Center for the Analysis of Violent Crime. That led to a pretty strong alliance actually that continues to this day. So we know that we can geek out on bombing, on bombing technologies and fusing mechanisms, and so forth, to a degree we can't necessarily do with other people.

Yost: And did you start attending the University of Alabama Birmingham right out of high school?

Bace: I did. We weren't certain; that was the biggest accident in my serendipity. I have a favorite lecture I give to kids from that area of the country on the power of serendipities and I point out to them that despite the best efforts and the best intention of guidance counselors that a lot of times life ends up being a lot more nonlinear than they ever allow for. (Laughs.) So I went out (in life) expecting that I would do something, you know, classically Southern woman; and first had epilepsy, and that was in adolescence. And at that point in time the attitude of the local populace was that that should be a major life-long disability. And I didn't quite get that. (Laughs.) I wasn't quite ready to write things off. And secondly, my father went through a business collapse. His employer basically went out of business. We were suddenly almost penniless so that kind of shut another door in terms of how fundable I might be in going to college. And sort of out of the blue; and sort of a one-two punch; I found out within a period of about three weeks, that I had won the General Mills state competition. I had taken a test; won a state competition that

awarded me a Minnesota-based scholarship that wasn't enough fully for school but was enough to at least get me started. And about a week later, the Teamsters Union gave me one of the Jimmy and Josephine Hoffa Scholarships that they put up that year. Jimmy and Josephine Hoffa had actually given up a year of bonuses and directed them to set up a scholarship fund and I was one of the first recipients of that. So I went from having nothing to having full funding for scholarship. And my sister decided she was going to graduate school. She was furthermore going to graduate school at University of Alabama Birmingham, which would allow us to commute from home. So she took over my transportation needs and away we went.

Yost: And did you have an idea of what you wanted to study, what you wanted to focus on at that time?

Bace: I'd always assumed before the epilepsy came up and served as a disqualifier that I would be a physician. I was always enchanted with medicine and thought I'd be a good physician; and found when I got to college that that was an automatic disqualifier for medical, any kind of medical profession. So I had worked part of my way through high school as the library assistant and thought oh well, I adore books, I can handle the library scene really well. I'll do some variation on that theme. And they had just set up a medical records library program at Alabama and I enrolled in that. One of the requirements for that was I had to take pre-calculus and for everyone that was "the course to dread." I walked into pre-calculus, I sat down; had a spectacular instructor; an unusually well-versed full professor just happened to be teaching that course that year and I promptly fell

in love. Went back to the guidance counselors at the university and said I'm looking for a major where I can take more math. And I still remember the stunned look on the face of one of them, saying "I've been in this business for 20 years and this is the first time anybody has ever come in that door and told me that (laughs); asked for more math." They said, "Well, as a matter of fact, the token woman in the engineering program just graduated and they've been looking for somebody else, why don't you go talk to them?" They literally marched me down and introduced me to the dean of engineering. And the next quarter I was an engineering major.

Yost: And what year did you start at UAB?

Bace: That would've been 1973.

Yost: Did you complete your studies there?

Bace: No, I went through a disconnect; I'd finished most of my courses at the end of like two-and-a-half years. I was well into my senior year and I could not get through engineering thermodynamics, which I needed to graduate. I had done a fair amount of a civil engineering degree; I had also done the better part of a math major; and could not get through the engineering thermodynamics. So, at the same time, at that point I had burned through a good bit of my scholarship funding and needed to work, and was teaching an engineering lab and a couple of fellows in the lab worked for Xerox and said "well actually, we're looking for a token woman. (Laughs.) We're in deep trouble right

now; why don't you come and apply? We're actually going through a hiring cycle." And the thing that converted me was that if I went there; that Xerox had one of the most generous tuition assistance programs. So they said, you know, piece of cake. You can go; you can work for them; they'll pay you decently; much more decently than you're going to be paid pretty much anywhere else. There are a lot of add-ons to the job you'll find extremely appealing and they'll pay your tuition as long as you want to go to school. So it struck me as being a good opportunity and after working a smattering of other part time jobs, I decided that was not a bad way to go. So I marched over to Xerox and took the test. Turns out I scored the best of that applying pool and ended up hired, so I was the token woman in Xerox's technical force for Alabama.

Yost: So you were hired as a field engineer?

Bace: As a field engineer; sort of a technician…

Yost: …going out and servicing the machines…

Bace: …servicing machines. (Laughs.)

Yost: My uncle did that for Xerox in Washington State for 20-some years and enjoyed his career.

Bace: It's not a bad living. I had a company car and the fun thing was they put me onto a particular line of copiers that were giving them a great deal of grief because you had, in order to troubleshoot, what needed to happen, you had a cage of computer cards and you had to be able to read digital logic diagrams, you know, and basically work through "and" and "or" gates to troubleshoot the problem if you had any kind of control malfunctions. And that was not a strong point. The rest of the fellows were far better with their hands and with the wrenches and so forth than I was in the mechanical end of things. However, I could basically seamlessly look at the logic diagrams and make sense of them in a way that they couldn't. So I ended up being kind of a control system person for them. It was a sweet arrangement for a while.

Yost: Back at UAB, did you have any exposure to computer systems as undergraduate?

Bace: At that point, I still remember they were so excited because they had gone up to - I believe it was - a megabyte of main storage in the main campus computer. It was a huge accomplishment and the system occupied the better part of a city block. It was a big IBM system. I took a couple of programming courses that were more business oriented, and took them sort of as a general studies, to fill out my general studies requisites; FORTRAN programming, and found it just amazingly, appallingly easy. I got somewhat adept at using a keypunch machine, another thing that we joke about as a group. It kind of marks you in terms of a generational group in computing. So I had that, and considered being a computer science major, which was, at that point, not legitimized, was not a legitimate major but was sort of a cobbled together hybrid between the math department

and the business department. I didn't really find the courses of interest so I continued in the engineering realm and took on additional majors, as they pleased me.

Yost: Can you expand on this?

Bace: I went actually a little bit laterally. I got fascinated with economics, and econometrics, in particular. So I did some aspects of quantitative modeling. Also, it kind of fleshed out the math courses I was taking so I got more heavily into differential equations and some of the Bayesian analysis, and stuff like that was applicable to electrical engineering. So I was sort of like on a grand shopping tour of the academic realm. (Laughs.)

Yost: In the early 1980s did you transfer from Xerox in Alabama to Maryland?

Bace: Well, in the early 1980s; I guess it was 1980; I had a situation with Xerox in which I was given the opportunity to leave Alabama. I would say Alabama was not the friendliest of political environments for me—you know, token women—there is blessing and curse in that, and I had managerial problems that were local to that area. And one of the things that was offered was a chance to leave Alabama. Well, in the midst of this, I got sent to a training school in Virginia, and there I met someone who ended up being my husband. So we were assigned at the last minute to a class neither of us was actually scheduled to take—we were last minute fill-ins for other people—and we met. He was posted to Baltimore. So when I wanted to leave Alabama, he says "well just come here."

So I transferred into the Baltimore office of Xerox and worked for a while here. At that point we decided we probably should get married. And at that point I also decided I should decide what I really wanted to major in and finish my undergrad degree. So we married, and that first year I took care of my mother-in-law, who was terminally ill, unfortunately. And then at night I finished out a data processing, computer science degree at one of the local colleges.

Yost: That's Regents?

Bace: Yes, I went through an aggregation program at Regents, but I actually went to a couple of the local facilities in the Baltimore community college system and rounded out the degree-specific things I needed to qualify for the degree.

Yost: After completing your degree, was the National Security Agency your first job out?

Bace: No, actually I worked briefly as an IT person for a small civil engineering firm. It was very logical; I had majored in engineering, I had concentrated in civil engineering so I knew that realm pretty cold. There again, it was total serendipity. A bad economy, so the job market was just stone cold and I had run across a woman who was sort of cobbling together her daily bread by doing placement, just cold call placement. And she had gotten a call from someone who was looking for somebody who had expertise about IT, ancient IT technologies, as well as civil engineering, and they wanted someone to

help out their IT guy as they made a conversion from an ancient machine into a much more modern piece of computing technology. So she calls me and says this is going to—I had not heard from her in months — and she calls me out of the blue one day and says this is going to sound crazy but I think I have a job that you might be well qualified for. And by the end of the day, I had a job. So I worked for them, but while I was looking for a job before then, I had come across a full page ad that was advertising jobs in the Baltimore-Washington area for folks with particular credentials, in particular, technology credentials. Didn't know who they were. Full page posting in *Byte* magazine, which was one of my guilty pleasures as a geek. And I applied. Sent my resume, looked at the posting again and realized that my husband, who was still working for Xerox at the time, also had credentials that would apply. On a whim, I sent his resume along with mine, and it went into dead silence. Well, after I went to work at the engineering firm, we got a call and a letter saying "we'd actually like both of you to come in for interviews. "And before I knew it, he had a job offer, and then close on the heels of that I had one as well. So when I got mine, my husband was ready to do something different from being a technician at Xerox. He had finished a master's in engineering and was bored so he entered the Agency, I think, in January of 1984. And I was getting pretty comfortable at the engineering firm. It was close to the house-we had bought a new house at that point - and I kind of liked the community. It wasn't paying a whole lot of money but I didn't care; I've never been really motivated by the money. And I still remember to this day the argument my husband used (to get me to accept the Agency's job offer); he says "you've got to work here"; he says "you'd fit in beautifully." I said "how's this?" He says "you remember these people we went to school with who, on the one hand, could do really

difficult differential calculations in their head in real time, but on the other hand, could not chew gum and walk down the hall without running into the wall?" "Yes." And he said "the place is crawling with them, he said, you have to work here." (Laughs.) For whatever reason, that converted me so I accepted the offer and went to work a couple of months after him and away we went.

Yost: Finishing up your education at UAB and Regents, did you have any exposure at all to the area of computer security or did you focus on a particular area of computer science at that time?

Bace: I was much more into looking at things from a microprocessor/microcomputer level. It's the fascination with *Byte* Magazine. In subsequent years I got to chat with Carl Helmers - who was the first editor for *Byte* Magazine. And I laughed and I told him, I said "this was all your fault. (Laughs.) Had you not published this; had you not had this particular ad, I'd never have done any of this." He would tell the story of the (government folks) having come to him and placed the ad and it was just hysterical. It was very, very funny. There was very much the cloak and dagger feel to the transaction and he was still rolling his eyes over how weird an experience that was. But he laughed and he thought it was absolutely hilarious that that one ad was enough to drag me into the intelligence community. (Laughs.)

Yost: What was your initial job title at National Security Agency?

Bace: They hired me in actually as a programmer, and I subsequently went on; I switched; went from that to an analyst, a computer analyst post. And then worked on, and got a degree in systems engineering. And at that point, took the additional course work to qualify, in the agency terms, as both engineer, as well as a programmer and computer analyst. So when I finished my master's I was dual certified in both of those disciplines.

Yost: When you first went to NSA, what was your initial impression of the organization?

Bace: Oh, I thought it was a horrible misfit. [Laughs.] I went into an organization where I was considerably older than other people; I was at that point, what, 28; and pretty much everybody else in our entry class was younger; so I'm an analyst and you go into an entry class and they wait on your clearance, if your clearance hasn't come through; wait for that to go through. But also you go through a series of indoctrinations so you understand all the organizations of the agency; you understand all the really weird rules surrounding what you can and can't talk to people about. There's just a whole lot of things you need to know in order to be a part of the organization. It takes a nontrivial period of time.

Yost: How long did it take?

Bace: Oh, months; you know a couple of months is not atypical. And it's fun because you get these (social) dynamics. You have these classes, entry classes; and the members of those entry classes, in a lot of cases, were friends for your career. People would talk about their "date"; their entry-on date classmates and enter-on duty classes; and they sort

of felt you should get to know each other as you come in the door. So I think there were three of us who were older than the standard entry folks in our class, and we actually still deal with each other; we're still good friends this many years later. But when I got into my first operational assignment, it was an organization with a system development effort already underway, and I was by far the oldest person on the team. And I was also a junior person on the team; had not gone to the same school as everyone else on the team. And I really, really struggled with finding a place on the team and had a pretty rough time. So I was ready to walk away. I had a team there that wanted me to go away; thought I was absolutely a horrible person, horrible choice. The only problem is I had developed some friendships with people who were significantly senior to me. They said, this is just a misfit. There are other places you might fit better, let us cast about and see what's there. And they found there was one group that needed somebody to do a very specific programming task, and it was a lot more complex than other things that were typically on the docket for a new programmer in the organization. So they sent me down the hall on a temporary assignment to work with them, with the understanding that we would determine if I would stay at the end of that assignment. And it was fabulous. Very, very bright people. One fellow who was a star member, was so humble (and humbling). He basically got - the first week I worked with him—I think it was a Monday or Tuesday—he got awards for his 25th and 26th patents. I think on Thursday, he got his Ph.D. And on Friday, he like turned 30. (Laughs.) It was just an amazing, amazing team of characters; and he's just a very interesting character. But I did some work for them. It was in a cool area; at that point, a bleeding edge technology area. And that was that; I ended up with an award out of the work I did for them. I was blessed as being worthy of hanging around.

So at the end of that, I interviewed subsequently for another job, building systems for the operational front and away I went. That was sort of my first five years with the agency.

Yost: What was the team working on with the operational front?

Bace: That was classified. I'm not at liberty to talk about what we were doing there. Suffice it to say that we were doing operational systems.

Yost: Were you aware of the National Computer Security Center within the agency at that time?

Bace: A couple of the folks that were in my entry class were headed for the National Center and I would meet up with them for lunch every now and then, and sort of slowly but surely got to know some of the folks over there and became good friends with some of them. Started building out a presence, at that point. But another irony is that I kept telling my husband, you really need to work in that; that's the area where I think you'd be well suited. He tended to make better sense of a lot of the security weirdnesses of the agency and the classified world than I did, and I kept telling him "I think you'd be a natural" and he was like "yeah, yeah, yeah," and was not particularly motivated to change. He wasn't going to do that; he was a good signals engineer, he was going to stay a good signals engineer, and that was that. So the irony was that I would be hanging with these guys socially, and chatting with them, and telling my husband "you really need to go over there" only to end up there myself. But in that first five years, I had a son and we

found when he was a couple or three years old, he was having developmental problems and he was part of the first wave of the autistic kids we see so many of these days. And as an encore, we got the diagnosis and all of that nailed down as well as a placement, early childhood (special education) placement for him, which was hard to get in those days. And literally, we finished that, we went on vacation, and ended up terminating the vacation a little bit early because he took ill. We couldn't figure out what was going on with him. Brought him back, took him to the pediatrician, and then went directly to the emergency room with a diagnosis of leukemia. So we came back from, we basically had done the autism side, you know, only to be, two weeks later, in intensive care doing exchange transfusions. My son had a very, very hot case of lymphocytic leukemia, and the treatment of that pretty much subsumed our lives for the following five years. So we worked through that and that became sort of the omnipresent "other", the other part of my life for those years because I was dealing either with his autism or dealing with his leukemia and it seemed that the autism would expand to occupy any space freed up from his leukemia treatment and vice versa. So that sort of tempered us, I think. It was a very interesting; it made for an interesting set of other exposures, as well. I think it made me think a little more expansively about general problem (and solution) spaces than I might have done otherwise.

Yost: How did the computer misuse and anomaly detection research program get started at NSA?

Bace: I think that it was started, actually, originally; the original seminal work came out of the earliest of the National Computer Security Center's work. The fellow who wrote the seminal paper for it, is Jim Anderson—the venerable James P. Anderson—who is considered one of those seminal folks in this area. Jim wrote the -Jim did the original work that made up the underpinnings for The Orange Book in The Rainbow Series. Jim is a fascinating, fascinating guy; also an extremely powerful mentor to me. I got to know him later on. Anyway, I guess it was in 1980 when Jim was inspired by a conversation he had with one of his neighbors in Pennsylvania; a fellow named Joe Wasserman. Wasserman was assigned to head the group at Bell Telephone, when Bell Telephone decided to computerize their business systems in the 1950s. He was the guy who was assigned to oversee the question of whether they should have an audit mechanism in that system, and they decided yes. But also, he posed a question to Jim as to whether there was security merit to the notion of doing something with that audit trail. When I subsequently wrote my book on intrusion detection, Jim gave me pointers back to an article that Wasserman had written in the mid-1960s that I cited in my book. So it gave me the gift of being able to nail that seminal piece of thinking down. Anyhow, based on his conversation with Wasserman, Jim put forth the premise, as well as a straw man, for the article that most people consider the seminal work for intrusion detection; article dated, I guess, in 1980, that he did originally for the Air Force. And then Dorothy Denning and Peter Neumann, at SRI, said "knowing what we know about AI type and higher level analysis games now, I think this might be a very interesting thing to apply to this particular problem" and she came out with a model that still stands as fundamental to

intrusion and misuse detection. They built that four-part model and we may have scratched the surface on three of them.

Yost: So it was Dorothy Denning's and Peter Neumann's work that was the earliest known application available to intrusion detection?

Bace: Yes. And I believe that the funding came from DoD and the NCSC; NSA is an executive agent for funding in those security realms. I mean, the way the things were, at that point, where they were sort of the agents for the funding the DOD set aside for security related purposes. So, Jim's work was funded, one could argue, by NSA. It's overseen by NSA. And I think, similarly, Dorothy and Peter's [Neumann] work was also under it, by DOD. I think more directly they're with the NCSC.

Yost: So while the DoD was funding a lot of computer research through ARPA/DARPA, they were also funding some through NSA, on computer security.

Bace: Right. Some of the smaller and frankly, some of the lower level of abstractions, some of the more specific topics were overseen and with funding that went through NSA.

Yost: Do you know what year the SCMAD research program got started?

Bace: Well, my team changed the name to CMAD. It was originally known as intrusion detection, I took it on, it would have been 1989-90 timeframe, when I changed from an

operational post over to the NCSC. Things were kind of in flux, at that point. So anyhow, when I got to the NCSC, there was an intrusion detection program; the group was headed by a very theoretical mathematician who was seriously into formal methods. And the general thought at that point was that formal methods were going to save us, all we had to do was just give up these damn programming languages as a means of building systems. We needed to have a formal way of designing, specifying, then generating the code in those operating systems and that if we did that everything would be perfect and life would be rosy, wouldn't have any more security problems. And, of course, the commercial computer world says, "are you kidding?" And kept on marching. (Laughs.)

Yost: That strict mathematical model of security?

Bace: Oh yes, the strict mathematical model.

Yost: to achieve "high assurance."

Bace: Yes, I had a fair number of folks I worked with who were absolutely, positively convinced that operating systems, that codes that were basically commercial languages, C language at that point was a big deal, but; the Cs, and the FORTRANs, and the PASCALs, and other programming venues were simply going to stop being used; they were going to become obsolete and if you could not do formal expressions, then by God, you were going to be out of a job. There was not going to be such a thing as a "code cutter" and anything resembling a standard programming language, you were going to be

sort of an assembler that followed from a mathematical expression, from mathematical model.

Yost: The threat posed by insecure systems would be the impetus for this change?

Bace: They thought that (the formal approach) would cure it; that it would cure the (security) problem and that would be a powerful driver. And I would do this, and then I had this deficit, in that I would actually go out and deal with the rest of the technology world (computer and software industry). The rest of the world would be looking at me like "what on earth could you guys be smoking?!" (Laughs.) "There's nothing today." I still have a nasty habit of reading books about technology communities, in particular, microcomputer and programming venues and platforms, and developer platforms. So looking at things from a commercial perspective, it was clear "something is not quite matching here." Well, reasonably early on, I started hooking into the academic circles outside the agency, as well as commercial circles in a quest to make better sense of what I was seeing around me. Folks decided that Gene Spafford and I had to meet. So they got us together; he and I just hit it off, I mean, just immediately. And it was obvious that "Spaf" knew his way around the formal side of computing, so he could speak; basically, he was a language bridge for me so I could come in and play "old girl from Alabama" and say "you know, this doesn't make sense to me" and he would say "oh, let me help you, I can catch you up with this," banga banga banga. I was laughing; I said, "okay, this guy's going to have a test (in helping me understand this); there's a test on this forever. And I said "this is what my boss is telling me about formalisms and (what) I'd like to

have (with regard to understanding);" and he says, "I've heard nothing but that," for the past 10 years. So starting in my graduate school, he says, "that horizon, that five-year horizon, that's constant." (Laughs.) He says, "I think it's been that way in perpetuity." So he says "you can believe it if you like, but put it in the proper category and don't consider it commercially actionable. If you want to do something useful in the commercial realm, you may want to consider another life message (besides using formalisms to secure systems) to march to." But this marked a start of a different way of tackling intrusion detection for me. First off, I started making the rounds and using traveling, the social networks, which I know how to do; I mean, it's a Southern trait. It's between Southern and Japanese; the convergence of the two makes it even worse than a double shot. So I started traveling those social networks; this person said "you really need to meet that person," and would subsequently introduce me to them And I got a pretty cool footing in the (professional) network, particularly people who have an interest in computer security but who also had established reputations as hotshots in computer science, in general. But (I) also (looked) for folks who have had good experience in the commercial realm; who had actually done entrepreneurial things in commercial realm; and I built an interesting network of those people. We were all kind of like-minded; we all got along beautifully. We also were good friends, but also shared a common vision that perhaps what we were working on in the intrusion detection realm was something that would be of value to the commercial realm and would be something (of value) regardless of whether the formal guys got their world view (implemented), you know, at some point in the future. We believed that in intrusion detection, there was something that would retain some value; that had enough strong basis in other disciplines beside the purely technical ones, so that

there was merit associated with moving forward, making an investment there. The other piece that became apparent was that the stories surrounding intrusion detection and why you wanted to do it were powerful enough, to have real promise in actually transitioning into operational use in the commercial side of the (computing) world. There was enough; you could assign monetary value to it a lot more readily to it than you could other areas of security. So away we went on an amazing march.

Yost: So you're doing research, but you're also running a program that is essentially building partners and networking with the academic university community to advance this area, intrusion detection.

Bace: Yes, pretty much. I wasn't doing that much in terms of the hands-on technology research. I understood it, but I found that I most enjoyed building that community and fleshing it out. So at that point, it (the research community) was functioning. I was teased from that point forward that I was actually doing the functional equivalent of an entrepreneurial CEO who had been given *vitro* funding and told to go build something in a particular area.

Yost: Another parallel with ARPA IPTO's funding, it was clear fairly early that a lot of the research could have important commercial applications.

Bace: Indeed. And I hear parallel stories. I mean, Jim was a very powerful mentor to me at that point; and Bob Abbott became, as well; we made that linkage. But the common

link there is that Jim had done similar things at Burroughs, as he was head of research at Burroughs, and was atop a similar model of tech transfer; translating research and re-bridging research to make a business stronger, to move the business and the industry forward. Abbott was very much on the same page. He did basically; he did pretty much the first really viable commercial practice in security, coming at it from an EDP (Electronic Data Processing) audit angle. We'd sit down and compare notes from time to time, and it was extremely clear that there were a lot of commonalities in our experience and our world view of what we were trying to get done here (were similar). So it was; we were fast friends, but also it was an extremely powerful alliance for me. These guys knew what I was doing.

Yost: So, Jim Anderson is one of the fathers, or "The" father of high assurance in that mathematically proven operating system, or a kernel of operating system, model, but he also saw other potential, perhaps more immediately practical, avenues to pursue in computer security.

Bace: Indeed. The blessing with Jim is that you would find (others in the security community) who would get extremely ego-involved (in ideas they'd put forward.) It reminded me in some ways, almost, of religious arguments. They'd invest everything in it (their theories) and any attack on the thinking or any challenge to the thinking was (taken as) a personal insult. Jim was just refreshingly free of all that. Jim's attitude was that if you'd gotten something; "if you take issue with something I'm putting forth, I want to hear about it; let's talk about it. You know, I understand I don't know it all. And if we

can argue about it, and I come away, I'm likely; I know that I will come away understanding things a little differently." "And chances are after the argument, you'll understand where I'm coming from a little bit better, as well." And being privy to that (ego-free message), it was an absolute treasure for me. Unfortunately, there were a lot of folks from the other camp, as well, who were very much "this is what you're going to buy into and by God, I'm going to do everything within my power to make damn sure you lockstep here with what I'm thinking." When you're trying to deal with something that's as pervasive as IT, (such restrictive thought) is a fool's errand. You have got to respect the scope (of IT); the scope both currently as well as future of the domain. That was sort of where I found it amazing that he could have that range of contribution and effect; but also was very respectful of (his limits) saying that, "you know, I think I've done as much as I can do with this piece of it, let's look at another domain and see what can happen there."

Yost: In terms of the intellectual origins of intrusion detection as a field, in your book you mentioned in the mid-1970s the RISOS project, and in studying operating systems to better understand security problems. Can you elaborate on that project and the impact it had?

Bace: It was; I mean, it predated a lot of the official interest in security and I thought it was fabulous in that it applied a good mixture—and it wasn't a particularly common mixture—of academic rigor and more practical notions. So you get the academic rigor and the hands-on, pragmatic focus. So you had a group of contributors who had a foot

planted firmly on either side of that divide and it was useful. You had folks who were adept at how people actually cut code for those operating systems and the design decisions made in those operating systems. But because of that, they could come up with a coherent way of classifying both the design errors, as well as the implementation errors in a way that allowed you to build out the (security vulnerability) lexicon in useful ways. This focus on doing RISOS well is we thought that people would get so overwhelmed with the more theoretical discussions of design flaws; a lot of the folks who were in a position to most readily correct the problems, would get so overwhelmed with the theoretical gyrations that they would tune out and basically say there's nothing here for me and walk away. And we didn't want that to happen. We thought it was silliness for us to continue to have pervasive issues when we didn't bother to try to tackle them with those folks who were best positioned to correct them. It just rankled my farm girl sensibilities. (Laughs.)

Yost: What about the impact of the 1977-1978 National Bureau of Standards meetings between government representatives and the commercially-oriented organizations?

Bace: I'm told that the primary value from the folks I know that were participants there, it was useful in that it allowed them to get on the same page where they could. I think it highlighted areas where perhaps we're (different factions within government and commercial worlds) never going to be on the same page. (Laughs.) But it allowed them also I think to see and have a much more expansive view of the landscape that we're going to have to tackle in order to make progress in this arena. And (the series) created

the basis for a lot of relationships that I think produced good collaborations over those years. I teased Bob Abbott; I came across a picture that they took at one of those meetings and I was absolutely howling; knowing these guys 20 years hence. We teased Abbott about the Afro for years and years and years. It was pretty; have you seen the picture at all?

Yost: I haven't.

Bace: It was absolutely… I ran across it when I researching my book. I ran across it in the University of California Santa Cruz library and it was unfortunately being quite noisy in the library; I was laughing my rear off. It was just too funny. I recognized more than a few people around the table. (Laughs.) It was just in a forum I never, ever; I could never in my wildest dream conceive.

Yost: Back in 1970, with the outcome of the Defense Science Board Committee's work, the report that Willis Ware wrote, one thing that he emphasized in that report—that overall was primarily trying to define the problems rather than offer solutions—was the importance of industry, the importance of keeping things in an open, unclassified environment so that industry could come along and help develop technologies and help foster solutions. What sense in your early years in leading the CMAD program; what sense did you have that that—looking to the commercial community—was a goal and an idea that was fostered within NSA, or was there a very heavy bias to doing things more internally?

Bace: Well, at that point, at that point, NSA would talk a good game and I think were well-intentioned but weren't really doing it. I found that we (the CMAD researchers) were making inroads into the commercial realm in ways that they were simply not accustomed to doing. A lot of this is, there again, a matter of world view. I think folks want to believe that if you're inside those fences, you can have a totally expansive world view; first, regardless of where in the organization you reside—totally bogus—and the other piece of it is I think there's a tendency to want to believe that what you see that goes under a particular label is all there is. So I think they would say "I'm dealing with industry", when in a lot of cases they would be dealing either with government contractors, who are not general industry (players), or they'd be dealing with the federal divisions of an industry player. So that limits them to dealing with organizations of a particular size; so an IBM, or something…

Yost: or a CDC or UNISYS?

Bace: Right, who are big enough to separate their main finances from anything that has to do with federal government because of audit standards. So, therefore, they have a federal division and the federal divisions going to be all over the federal agencies in hopes of generating massive sales and so forth. The agencies would see these guys coming in; these would be the only people they'd see coming in, and I think there was a tendency for them to say "that's all there is to this particular firm, I'm seeing them all"; whereas the commercial realms were in another dimension entirely. And I, almost by accident, ended

up increasingly getting to know those who were working on the commercial side. And I was getting a real different view from most of my colleagues so we would have interesting arguments over this difference. (Laughs.) But it was still quite different. It was, in a lot of ways, a real pleasure to me because it allowed me to see where we (our technology) worked, where we weren't connecting (completely), and weren't connecting at all. But also, none of it was intractable, where you could actually sit back and put on your program manager hat and say okay, if I take these steps and in this period of time I'm going to be able to deal with at least the worst of these obstacles (to deployment) and be in a better place (than before). It won't be on the federal budget's, you know, three-year cycle; but three years from now we'll see measurable progress towards actually having a productive conversation with these characters.

Yost: Earlier, you mentioned Dorothy Denning and Peter Neumann's work in connecting the idea of an expert system with intrusion detection, which resulted in the Intrusion Detection Expert System (IDES). Can you discuss that system and its early impact, on how it might have influenced other broader developments in the intrusion detection field?

Bace: Well, they weren't unique, in terms of doing work in that arena. Their advantage was that they (along with plenty of others up until then—I mean, this is pretty much how Anderson was thinking about it, as well)—were thinking about intrusion detection as being primarily an expert system. And where the advances were made in their work is that they added an analytic component, saying okay, we can use a little bit more pure analysis, looking for (statistical) deviations in behavior, and at the larger, different levels

of abstraction, as opposed to doing the expert system that would replicate simply some sort of a manual (checklist) audit sort of process.

Yost: Was this more dynamic?

Bace: Well, they were in a position where they presumably could recognize Zero Day, what we know now as Zero Day attacks. So you wouldn't have to have foreknowledge of a particular attack to be suspicious; you could spot anomalies and you could say "okay, this is unusual and this warrants additional scrutiny." And they saw that as a key to being able to do monitoring that was useful over time. Otherwise, you limit it strictly to a fixed pattern, particularly a fixed expert system template. People weren't thinking in any dynamic terms, at that time. If you're using an expert system; if I were a hacker coming in, first thing I'm going to do is I'm going to access and learn that expert system cold, how to reverse engineer it and then devise a kagillion attacks that step around the cues that the expert system looks for. There was a project that was actually implementing these sorts of things on the expert system side that Tom Berson was doing at—I was trying to think of the name of his firm – ARCA Systems.

Yost: Would you spell his last name?

Bace: B-E-R-S-O-N. He should definitely be on your interview queue. Tom's done a lot of really significant work; but he also is one of the first financially successful entrepreneurs (who came from the security community) and he made a fortune; he did the

firm that did the original transmitters for the cable television industry and had come up with other advances. He was extremely; just a delightful guy; he's in Palo Alto. I think he sold his holdings to Hughes for maybe the mid ten figures, early on. So he predates the classic Silicon Valley dotcom characters, by 10 years. But Tom had a security-centric consulting firm that did products for the community. And Teresa Lunt, who ultimately took on the mantle of program director for the IDES project—which started with Dorothy and Peter's stuff—worked with him. I feel like it's not; it may have been ARCA Systems, A-R-C-A, at the time. She and Bill Wilson, who is likely also on your queue, I know were there at the time. Another woman, Liz Sullivan, was there as one of the earliest formal methods expert practitioners. But ARCA did a lot of early contract work; small firm; and I believe one of the things that they did—that would've been in the publications in the late 1980s, maybe 1987, 1988—was an early intrusion detection system, misuse detection system. I think Teresa was one of the primary designers of that. So Teresa went from there to SRI to handle IDES shortly after they did that system, published that system. IDES was funded through the Navy but there, because of the way funds flowed through the DOD, it went through me first. The Navy was part of my line item.

Yost: I'd like to go through each of the early university centers or research groups that you funded with CMAD and have you talk about them a bit. You mentioned Spafford at Purdue with the COPS project. Can you tell me about that project?

Bace: We chatted originally; one of his [Eugene Spafford] Ph.D. classmates at Georgia Tech had done work for me; and introduced us. I think at that point, Spaf had either just

gone to press or was about to go press with the first edition of "UNIX Security" (the book he wrote with Simson Garfinkle.) And as I said, he was one of the first folks that actually made sense, you know, to the farm girl half of me. But also I thought that—it was an extremely popular book at the time—I thought there was a certain clarity in his messaging, plus his approach is very pragmatic; you know, "we have this obstacle that's considered a major pain for the commercial world, why don't we tackle it and move on?" But I thought that was a compelling vision to have things (pragmatic, yet) correct from an academic point of view. And this ended up violating all sorts of symbolic strategic goals and self-images that had been put forth in the Computer Security community. This was one of the wake-up calls I got from Jim Anderson. Jim Anderson says, "you know I finally understand why you're raising so much ire politically at NCSC because we always considered ourselves to be a pure science, not an engineering engagement and", he said, "what you're talking about right now is just not theoretical at all." He says, "you're crossing the boundary into engineering." "However," he said, "I cannot dispute that you're correct and it's time for us to get up and do intrusion detection in the engineering domain." So Spaf was thinking about it in ways that looked a little bit more like a really good theoretically-rigorous engineer and I thought that his vision was good. He had a lot of energy; but also I thought that Purdue was probably not a bad place to place a security project; they had a good tradition, good track record for turning out folks who could do real things in the real world and make money doing it. (Laughs.)

Yost: Right. One of the leading engineering schools in the country; probably the best in the Midwest.

Bace: Indeed. Well, I think there that you look for; there are certain markers—we joke about this, you know, (when we do) the cocktail napkin reverse engineering scene—but it turned out, it seemed, that the best fit for schools to do that kind of effort were schools that were Engineering and Agricultural schools. So, technically, I should not be at University of South Alabama, I should be at Auburn where we have that overlay of Engineering and Agriculture. There seems to be a certain pragmatic streak in such settings that's very, very useful when you're thinking about security stuff. I mean, between UC-Davis and Purdue, I was very, very pleased with the payoffs that we got; the returns on the investments we got pretty much across the board.

Yost: Can you move on the security lab at Davis and your funding of research there?

Bace: Oh yes. And I need to point out, that work was already underway (when I arrived on the scene). Air Force had already made some investments at Davis. Tim Grance, who was championing intrusion detection research and development was already in place at Air Force, when I came in. Tim is a "lifer" as well –when he left Air Force, he went on to NIST; where he helped build out NIST's programs in the security area. But yes, Karl Levitt, who headed the security program at Davis Computer Security Lab at Davis; had, before that, been head of the computer science lab at SRI. He had been in security-related research since 1968 and remains a fabulous friend—I don't know if you've dealt with Karl yet—interviewing him will be an adventure – and extremely productive – I can promise you that. But he has got one of the most amazing histories, and intellectual

grasps at all levels, of the computer security realm. Serious, serious work ethic, as well. I mean OCD all the way. (Laughs.) We joke that you don't have to be OCD to be in this biz but it helps. But Karl was not only a visionary there, but also strong on all fronts. I think that Karl actually was not a mathematician but was educated as an electrical engineer; he had done all the work in the trenches in the formalisms, but Karl could seamlessly go from a formal descriptor of a pretty arcane system primitive into something that was tangible that I could take it as a programming task. He could (make this transition) in about a minute and a half (laughs) and have your head spinning for a week and a half later. I could sit down and talk with Karl, or be in a meeting with him, and I'd go home, and like a week and a half later I'd go oh! - and finally understand the point he'd made. (Laughs.) He's just that kind of a guy. Just a lovely person as well.

Yost: And was it funding you provided that lead to the network system monitor?

Bace: That would've predated me. The original network system monitor that Todd Heberlein did was funded I think originally by Air Force and other grants. We had some funding relationships where the money went from us to Lawrence Livermore, and then to Davis. The straight line relationship actually came in a little later, probably 1990-91. The NCSC had a mandated review of their program by a group of security "graybeards," you know, they were like the leading lights in security at that point. And they came back to the director of NSA with very specific recommendations. One of them was that "you guys need a university research program to keep you honest," and advised them to set up the funding. The problem was that nobody in the research group wanted to deal with it.

Why on earth would they want to deal with another outside entity when they could come to work every day and not have to deal with these outsiders who drove them crazy - furthermore, if they ignored these outsiders, they would not have to worry about the classifications and other security issues. Whereas I looked at it as found money. So the management set up a pot of funds that was designated, I think, from the director's level; and said "these are set aside for security proposals from university research programs, and these are the requirement outlines." I went to the folks I knew within the security academic community and said "I consider this found money. You have got really, really good ideas; let's write them up in proposals and put them in competition for the funds." So I think the first year that we had the University Research Program, my Intrusion Detection research program walked away with probably 60 percent of the funds, which was not what my management had in mind – they were seriously pissed off. However, I'd been out; you know, encouraging submissions. I had probably 25-30 proposals and the rest of the research programs in total may have had 10. So, you know, I got good efforts funded since I had been able to encourage my community to generate the proposals.

Yost: Can you speak about roughly the dollar amounts that were involved with funding these university-based intrusion detection research projects?

Bace: They were not that big. It's not big at all. I mean, you're probably talking about things in maybe $100,000 chunks, at the largest. It's just that you could have multiples. But the amount of return on that investment was immense. The Distributed Intrusion Detection system (DIDS) that came out of Davis represented a miniscule amount of

money, on government terms, but it laid the groundwork effectively for the industry; a whole generation of network-based intrusion detection systems.

Yost: So the work at Davis was the first application of the monitoring networks for intrusion detection?

Bace: Todd's work was the first I was aware of that involved surveillance at a network layer of abstraction. He did a pretty straightforward job of just setting up an ethernet connection in promiscuous mode and picking up the data stream. But there was a lot built into the system as well, in terms of deeper thought that wasn't reflected in the commercial realm for a while, for a couple of generations of products. So the work that went on there was just extraordinary in quality.

Yost: The early work of the Air Force was addressing the problem of systems in an open environment with multilevel users. Was the NSA a completely closed environment and did that influence kind of the prevailing thought about what was important with computer security?

Bace: I think that certain of the security projects were affected. The agency also did (an IDS) that was published in one of the early national computer security conferences. This was an in-house system that monitored DockMaster, the agency's first public access or outside access unclassified system. I know that the system itself is at the Computer History Museum in Mountain View. Anyhow, they did a program called MIDAS

(Multics Intrusion Detection and Alerting System), designed and built by an in-house team, that utilized a lot of the Multics data streams, and audit trails, augmented by other monitored data streams. Multics was a dream (operating system environment). Multics was an extremely rich example of how one might want to do a more secure system. A lot of work went on there but also a lot of folks who went on to do significant things in security (and in computing in general) cut their teeth in the Multics project, you know, the whole "Multicians" group and associated history is humbling, to say the least. (Laughs.) So the agency did MIDAS and I think they acknowledged that you need to be able to monitor and do IDS, you know, on a public-facing system. And (as it ran) on a commercial platform, Multics still qualified as a commercial OS at that point. But the Air Force was trying to go at it from a little bit more pragmatic operational point of view so I think the first thing I dealt with in IDS from the Air Force was Haystack. Haystack was novel, for NSA anyway, in that it wasn't dealing with a secure, or even an ostensibly controlled computer. It was an attempt to protect logistics computers, you know, operational logistics computers, which were as wide open to access as anything you're ever going to find in DoD. So Air Force was a little bit more expansive in their view of securing computing systems. The other thing now that marked the Air Force as different is that Ken Minihan, who ultimately was Director of NSA, was in charge of AF security. Ken Minihan cut his teeth as an information security specialist, from the outset. He'd done a couple of tours through NSA and Ken knew probably more about information security than anybody else in the military brass; knew this area cold, from the point of view of technologist. And Ken also was unusual in terms of the amount of operational risk he was willing to absorb, so he was instrumental to our making any progress at all;

he ran a lot of political, covering fire for the folks working on CMAD research. We got a lot more license in pursuing our interactions with the outside technology world, particularly with the academic world, than most folks would've allowed within military, particularly security-focused military, at that time. Ken and I remain good friends to this day. He followed me into venture capital. So he's quite successful, which is helpful, too; investing in good security products and services. So that's been a happy outcome; but I was also really happy to see him in a position of influence, because his view was so different from what was prevailing at the time.

Yost: The National Computer Security Center, was that NSA? But was it also partnering with DoD wasn't it? What was the relationship there?

Bace: The NCSC was part of NSA, which is a part of the Department of Defense. NSA, and subsequently the NCSC had widely differing attitudes regarding cooperating with external entities. Depending on who was in control at NCSC and what their thinking was, any external entities were all too often viewed either as folks to be bossed around, or else folks to be considered blood opponents, you know, competitors. I always considered that tragic. I think that some of these entities, especially NIST, has bloomed the last ten years in particular, and people are actually appreciating what they are doing. But they're doing what they were always meant to do in this area. They're finally getting a chance to show their stuff. Whether they're getting sufficient funding or getting sufficient political license, is another matter. But I like to see them doing well and having a real influence on the industry. At time when I was with NCSC it was torturous dealing with NIST. In terms

of the military, you would have folks that did tours who came through but most of the relationship with the military was almost adversarial, as well. You would have evaluation teams that came out from NCSC to evaluate systems and determine their security road-worthiness, as it were. You would have military personnel assigned to the Center and they were used primarily for those sorts of roles but it was hard to see it as a plum assignment and I think that there was a lot of potential for those relationships that was just never ever fulfilled. I had a deputy who was an Army major who had been retrained as a computer scientist after serving as a military policeman for much of his career. I absolutely adored him; he was perfect; absolutely great. As my deputy, he could make sense of a lot of things that were totally, hopelessly arcane to me; when I reviewed non-technology topics such as criminal law and so forth, it was perfectly clear to him. But he was also just a really good person in terms of working the liaisons with the various military entities. So I think that there's a lot of potential in the military; how much of it was fulfilled? In general I thought the military relationships with NCSC fell short of what was possible.

Yost: You mentioned the richness of Multics. Can you expand on how that influenced your thinking and what specific connections to intrusion detection were there with that time-sharing operating system and other associated work that was done at M.I.T.?

Bace: I think it was very interesting in that a lot; if you talk to folks about other operating system development, aside from IBM, folks outside that realm, you didn't really have that robust a competition amongst operating system platform vendors. There

were always going to be portions of the system that were there because some customer said they had to be there in order for them to make a buy. But there was never any assurance that there was going to be any kind of quality control or any kind of engineering coherence applied to it. Particularly in my domain, audit trail generation was one area that was notorious for these sorts of deficits. So what was cool about Multics was that from the outset, they designed and built in a set of monitoring locks and one of the most expansive monitoring arrays I ever saw. It's sort of like intensive care for health care, the more traces and vital signs you can monitor, the better the chances are that you can find a problem before it develops into something that's life threatening. Same principle at hand here, so it's a luxury to have such comprehensive monitoring mechanisms.

Yost: So Multics is far easier to monitor, as an operating system than IBM systems?

Bace: Absolutely. Subsequent operating system environments were less evolved in this regard. This led to an interesting side effect of the CMAD program. We had real success in placing pretty much every graduate of the CMAD University research programs in security relevant areas and one of the folks that came out of those programs ended up as head of an audit development team— (he was the team lead for audit design and then the development team)—for one of the major manufacturers. He later came back and said, "you know all these things we theorized might be wrong (laughs) they have these huge Mack truck sized holes in the design where they weren't monitoring critical events." "Remember, all of these things that they were purporting to monitor in the

documentation?" "There was basically no correlation between what was actually in the system and what was documented as being there." So one of the things that I thought was most fun; and actually, I think, one of the best returns we got (on the investment represented by the University Research funding) was to have funded Ph.D.s and master's degrees in security-focused areas, with folks who subsequently went to the operating system vendors and actually straightened this stuff out. This allowed the rest of the technology we were investing in to work. So we had a lot of instances of that sort of tech transfer, via person; via graduates.

Yost: With this migration of graduates, other systems gained some of the same or similar design characteristics of Multics?

Bace: As most were exposed to Multics (and the expertise that came from the Multics project) I think it a reasonable assumption that Multics would have informed their work. But this leads to another point worth making. I think people talk a good game about wanting to do tech transfer, whereas the irony to me remains that the most substantive tech transfer we ever did was to fund -and oversee- really good educational research efforts. Because if you did a good job of recruiting the right people into that educational program and got them fired up on the mission of securing these systems, they would be the folks who would go out and reinvent the commercial world. I mean, the commercial IT industry folks were all too happy to have these well trained security experts; they understood they were in deep trouble (in areas related to security) and hiring this crop of experts became sort of a no-brainer or the no-sales effort whatsoever proposition for

them. I'd approach commercial systems vendors and say "I've got this person with me; and this is their background; and we have grown them for the past three years to do explicitly this sort of security technology thing." And they were like, "how much money do they want and when can they start?" (Laughs) It became a rather ironic sign of success in the security education programs that were the hottest, (i.e., that were the most competently run) - that the biggest problem was keeping the kids around long enough to graduate because the vendors would be so hot to recruit them, degreed or not. So that becomes a very interesting, performance measurement mechanism. You know that you're doing such security tech transfer programs right when you are having that problem. That was also one of the biggest ironies because I think there's a tendency to measure tech transfer in terms of whether a dissertation or a thesis you underwrite ends up in commercial form as a product. But I think that the better goal is whether that person you educated to do that dissertation research ultimately ends up in a position of responsibility and power, influencing the commercial world in ways that improve system security

Yost: Much longer term payoff over an entire career.

Bace: Oh heavens, yes. Well, the other irony is that the (theoretical) product's leaving; you don't know whether the transferred product will be in common usage three years from now, after the next version or advance comes along, which may set you back awhile. On the other hand, the people typically stay in place for a period of time and (their contribution) doesn't flip back, you know, they both gain in wisdom and acumen,

but also educate those who come in their wake. So one of my pet peeves is that I believe people think about tech transfer with much too narrow a scope.

Yost: You also funded work at the University of New Mexico. Can you tell us about that?

Bace: Yes, that was very early on and that was primarily on the network side, as I recall; it's been a while. Barney Maccabe, the person who introduced me to Spaf. They'd done Ph.D.s together at Georgia Tech. Barney, I believe, later became the CIO for the University of New Mexico, the UNM systems. But back then, he and George Lugar were working more at the network layer with focus on monitoring and correction mechanisms.

Yost: So work somewhat similar to Davis?

Bace: Yes, but with some critical differences. They were focusing more on the routing infrastructure; they were at a deeper level of abstraction in the network realm. I also funded Paul Helman and to a degree, Stephanie Forrest. Their focus was on very, very innovative schemes for performing artificial intelligence analysis of data streams, looking for symptoms of security issues. Stephanie Forrest had put forth a real interesting approach to detecting attacks using biological, genetic algorithms. This represented a very novel means of looking at Zero Day Attacks. And that ultimately resulted in a classic tech transfer success - in a commercial product startup. Steve Hofmeyr, who did his dissertation research with Stephanie, exploring that approach, was CTO of the product

firm. The group at UNM were just fascinating people. UNM was not where I expected to find such security talent but there was a significant store of it there.

Yost: And Tulane?

Bace: At Tulane I funded Mark Behard and his PhD student, Linda Lankowitz. Linda was, in some ways, being an example of a successful tech transfer in human form I mentioned before. Mark's and Linda's research focused on using clustering algorithms for spotting abnormal activity on DEC and some of the legacy platforms. Linda was using clustering algorithms operating on DEC audit trails and other operating system outputs. So in some ways, she was implementing some of the vision that was put forth by Dorothy Denning in some of her original IDES research. Linda was going outside the realm of the early, rudimentary clustering algorithms that were in common usage at the time, testing them against more modern algorithms. And they were able to converge, I think, on a k-means algorithm-based mechanism that worked well.

Yost: University of New Mexico, Tulane, Purdue and Davis were the four you mentioned in your book. Were there other universities that that you recall that you funded influential people or research?

Bace: In those cases, there was a second generation who went out from those areas. So there are a fair number of those who I think were educated in those early efforts who ended up in places like Carnegie-Mellon. There are a few that came right after, right in

my wake, and then a future second generation. The second generation; a first comes to mind, where Deborah Frincke and Jim Alves-Foss, who went on to University of Idaho and did work there. Deb went on to a security startup and led the cyber research team at Pacific Northwest National Laboratory; and is now serving as Director of Research at NSA. So she's an extreme case, a real trooper, in terms of the tech transfer I was mentioning before. There are a number of those at Purdue who have gone on into other areas of academia; they are a little bit more internationally distributed, as well. I'm trying to think of who else is in the strict academic realm. There are folks who postdated investments I was making there. And probably a third year into the program, the rest of the organizations within the research directorate at NSA were catching on that they ought to be funding work. Let me take a break.

[BREAK IN INTERVIEW]

Yost: One area I haven't asked you about is that you talked a little bit about the culture at NSA. Can you talk about the culture with regard to gender? Was it predominantly a male environment?

Bace: I think so, yes. I mean, there were some orchestrated attempts, particularly in engineering organizations, to escalate the progress of women to management positions. But those were isolated, at best, and invariably I got pounded on a good bit, not so much in outright discrimination but for failure to conform to a model for "women" technologists. Such disenfranchisement tended also to be worse in certain organizations;

also, much depended on mission. Things have changed but mostly driven by more general social trends. Or if you find women within the organizations, you find them predominantly in support or administrative positions versus in-line mission elements. I'm seeing change to a certain degree, now, but it's still not to the degree we would like. But that reflects also a lot of trends and deficits in terms of the number of women we graduate from particularly science and technology programs.

Yost: And what about the broader research community at the universities in the intrusion detection research area?

Bace: We were reasonably balanced, I thought. One thing that was nice is that I think academic research was a friendlier environment. Particularly once one got out of the federal realm it was a much friendly environment for women to be in than certain other areas. Some of the harder engineering areas were a much bigger pain in the rear to deal with. We were decently balanced, but also, the gentlemen that we dealt with within the programs were so dedicated to their technical domains that I don't think many of them ever thought of discrimination against women being an option. The experience that I had over and over again is that whenever the topic of gender discrimination came up they would observe it going on in other venues we were in and be totally amazed that it happened at all. It's just like the thought had never occurred to them; which is lovely; that's the way it should be. So that part of things was refreshing. In the commercial world in general I'm seeing the gender bias decrease a little bit; in the development realm it's still there; women are still rather a rarity and tend to populate certain specialty areas more

than others. However, I'm seeing in security risk management, where much of information security is applied to the commercial world, has changed and changed for the better over the years. So there are a disproportionate number of women who get promoted up the ranks in security risk management now. And I'm loving it; every bit of it. We went through a period when things I did later on in my career was work to set up communities of support for women who were executives in the commercial side of security and risk management. And there was a period of time where there were a series of large financial organizations who, when they did searches for a head of global of security, ended up with women beating out nontrivial pools of male candidates. And that is sweet; I'm enjoying that.

Yost: Are most of the people that are doing security administration coming from a computer science, computer engineering background or is it also management of information systems, and other types of training?

Bace: It's a real mixed bag still. I think security has traditionally attracted folks, who are outliers – people who do not fit gracefully into other technology domains. And that's exactly who you want working for security. The quality of the security job you can do typically depends on your ability to master the domain you're trying to protect but also see that domain from a different point of view. So it's a matter of needing somebody who has a mastery of that technical domain, but also a certain oblique view of it so they can come in, look at the domain, nail the details of the domain dead to rights, and also notice what's not consistent as they observe operation of the domain. So in some ways, my

assertion is that you want those kind of people who color outside the lines, in this area because it is the place where all these folks best fit. But also, a lot of the traits inherent in these folks correlates to difficulties taking a linear path anywhere. This extends to difficulties taking standard routes through educational systems in general and in particular completion of degree programs. Some of the most gifted security folks I've ever dealt with have not made it out of high school, even though they were acknowledged as having technical qualifications and talents that would far exceed what you would expect of a graduate or somebody that's completed a terminal degree.

Yost: Do you have any that have a background as hackers or not?

Bace: Some do. I mean, the other thing that I think people confuse is the ability to examine a system for security problems, the ability to either build a system that is resilient or resistant to security problems, and the ability to correct those problems once found. And I found that those tend to be very distinct populations. And I think that, as Spafford's been saying forever, the confusion there is tantamount to this conundrum; asserting that a hacker is best equipped to correct security issues in a system or design a secure system, is like saying that the primary qualification for an auto mechanic for your car should be demonstrated excellence in putting sugar in gas tanks as a kid. (Laughs.) They're really different games. I think that confusion creates a great deal of dissonance - complications for the security area in general. (Laughs.) But also I worry that that confusion also interferes with doing good jobs at recruiting for areas that really badly need good security expertise.

Yost: I'm not sure you will be able to comment on this question, but did research in intrusion detection contribute to understanding how, essentially, to subvert adversaries systems, for intelligence gathering efforts; was there communication between those two groups or were they largely independent with NSA?

Bace: Oh, it was independent, and it remains independent, by charter and design.

Yost: Was that part of the NCSC?

Bace: The NCSC was created to emphasize the point that protection was fundamentally different from exploitation. Originally when I went to the NCSC, I went to the research group for the National Computer Security Center and that was always held apart from the research group for NSA. They did this because it was assumed that the research group for the NSA did hard fundamental research or else did research that served the operational side of the house. And when there was a move to reorganize the Computer Security Center, you know, shortly after I got in; they reformulated the research group into a separate research element. They differentiated between the operational, the research group that serviced the operational research crowd, and the research group that empowered the information security side of the house; acknowledging that they were separate missions. A lot of effort goes into keeping those separate. Fundamental to NSA is the acknowledgement that there are two missions; the two missions were put into the same organization, acknowledging there's a certain tension between them. I think that it

just became easier, after a point, simply to separate the two elements. You worry about cross pollination there.

Yost: Within NSA there is a very long history of COMSEC, and it's really later on that you've got COMPUSEC within NSA. Can you speak about the relationship between goals and priorities within NSA—between COMSEC and COMPUSEC? Were there equal opportunities for advancement?

Bace: I think the deal was a conundrum there in that COMSEC had the luxury of effectively a copper wire communication system, where you had the luxury of extremely specific devices populating the system and a very, very small number of entities controlling it. So that was the day of the Bell (telephone system), you know, and copper wire linkages, and a real strong separation between those who used the systems and those who managed the systems. The advent of computers, in particular, the advent of computer networks, screwed that all up. Boy, there's nothing to keep a user of a system from managing a system down to the bit level, down to the hardware component level. That's the essence of what hacking is. You know it's only a boring hacker that confines himself to the software, anymore. A colleague deals with kids who are 12 years old and mess around with firmware. I'm told they do it quite successfully and alter that firmware in ways I would never think to do myself. You know they've become the equivalent of me playing with dynamite at that age. (Laughs.) There's a kindred spirit there. Still, you're in a situation where we don't (technologically) stand on anything resembling solid ground anymore. It can all be tweaked beneath us. It's pervasive. We don't have that

surety anymore in terms of understanding what the biologic world gets us. But we certainly, and in particularly in communications, I think, end up being overwhelmed by the advances. It was a lot easier when it was a straight wire and you had, you know, "the gazintas and the gazouts," according to our friends. And you could scramble the gazintas and the gazoutaos and be reasonably well assured that you were going to have covered the landscape sufficiently. Now, you have no such assurance.

Yost: I'm trying to get a sense of the early computer security industry, and specifically intrusion detection within as a part of that emerging industry, in the 1980s. In the early 1980s you have the formation of RSA Data Security as a company and outgrowth of the research of Rivest, Shamir and Adleman at M.I.T. Did that company have an influence on intrusion detection or was that completely separate?

Bace: It was pretty much a separate domain. I think that there was always a strong separation of crypto, from what we (in intrusion detection) were doing. We were like an entry in the 'other topics as needed' column. So that became some of the awkwardness in computer security because it was obvious there were certain areas in which crypto was necessary. It was sort of like having a parallel universe. I have a lot of friends, very good friends, who are extremely good cryptologists but it's as if we worked in different domains.

Yost: Also in the 1980s, extending from—and actually a bit before in the late 1970s—extending from the work of IBM sharing of RACF and ACF2.

Bace: RACF and ACF2 actually had more in common with us. It was a little bit more of an overlay there, although what we did pretty much came up independent of what was going on there. (I've had) a lot of long conversations with Bob Abbott on this one as he was, of course, quite adept at both as part of his classic audit, EDP audit practice. Although in some ways, he was working yet another parallel universe to ours. There was a little bit more bleed over that had to do with policy; with the policy world and the compliance world.

Yost: In your book you wrote about Clyde Digital, briefly. Was that one of the first commercial contractors? Can you share what you know about that company?

Bace: Yes, they very much one of the first commercial IDS product vendors. That was a firm formed by Dr. Robert Clyde and his two sons. One of those sons, Rob, ended up as CTO of Symantec. But Clyde [interrupted]

Yost: Is he still there?

Bace: No. He stepped down from that post. He's still active in the security and startup world. The Clydes have always been Salt Lake City-based. And they—Clyde Digital—had a DEC-centric consulting and products business. They focused very much on DEC platforms and were quite good. But Dr. Clyde, the senior, I remember presented at one of the early national computer security conferences, and the graybeards of the NCSC, that

surrounded the NCSC, basically wouldn't give him the time of day. Their message was on the order of "Well, you know, he's not dealing with trusted systems so we don't want to hear about what he's doing; he's obviously behind the curve." And I think that was a source of considerable frustration to him. But Rob tells me that they had products in place extremely early. They had capabilities that were foreshadowing what we would do a decade removed, with commercial intrusion detection space. It's nice to have the luxury of focusing on a specific platform and in some of those cases, I think they were further confined to a specific application they used as well, that's helpful; non-networked, which is even more helpful. And containing the threat realm is very, very nice. But they had products in service early on; I think they had particularly in the EDP audit communities and so forth products in place in pretty wide usage long before other vendors were fielding products.

Yost: What about Tracor Applied Sciences and Technologies . . .

Bace: pronounced "Tray-core"

Yost: . . . they developed what became Haystack system.

Bace: Oh, heavens, yes

[Post interview comment…I did check this and my memory was wrong. Tracor was, however, the original perch from which Steve Smaha did Haystack for the Air Force.

They went under before he was finished, and he set up Haystack Laboratories in order to finish.]

Yost: You talked a bit about MIDAS earlier. Was that a project that was done entirely within NCSC?

Bace: It was. Within NCSC.

Yost: Was that a project that you were involved with?

Bace: I knew a good bit about it. I worked with them. There were some of the folks, in particular, Eric Shellhouse, who was one of the leads; and Mary Hanna was another. I'm comfortable talking about them because they published their results; they're coauthors of the paper that was ultimately presented probably around 1988-89 at the National Computer Security Conference. But they were a serious part of my learning curve for intrusion detection. They had done a beautiful piece of work. I was really, really impressed by what I saw. They actually turned me on to the notion of what it would take to build a coherent commercial argument to justify buying intrusion detection. They would say some of the most things you wouldn't think of first hand in terms of the value of having such a system. But one thing they told me was of giving them evidence as to the effectiveness of other security measures they would put in place. So they would say we could watch; the system gave me a way of being able to say okay, before you put this in place, we had this many approaches from these sorts of venues and this was the

success rate at actually penetrating this or that. You know, it all stopped when you put this other measure in place. So it became a way of being able to give you a notice of how your overall security strategy was working. I thought that anything that allowed you that capability was going to be a commercial success; it was going to be an easy buy to justify to one's boss if you're responsible for security and risk management.

Yost: It was to protect the DockMaster?

Bace: Right. It was designed specifically to deal with DockMaster.

Yost: How did that system compare with other systems both within the defense and intelligence communities, and outside?

Bace: DockMaster was a Multics platform. I think it was unusually well-managed security-wise; had a lot more monitoring on it and so forth. But because of the affiliation with the NSA it was also a much bigger target. So there were probably intrusion attempts that were frightfully frequent. But DockMaster was great. Among other things, it was one of the few things that actually yanked this computer security community as a whole into the modern age. It was by and large my first public e-mail address, I know. And I suspect it was the first prevalent one (email server) for many of the members of the security community. The way the rules of engagement for DockMaster worked was if you were a working member of the security community then you could apply for and get access to a

DockMaster account and e-mail address. So [it] had numerous forum[s] and that was sort of the place to be. It was a great deal of fun.

I think it was where many people really caught on to the power of electronic connectivity. They really caught on to why internetworked systems were going to be a commonplace trapping of modern life because they could see the power of it as implemented within DockMaster.

Yost: Was it a system that was rated within the TCSEC certifications?

Bace: I think so, but I can't remember what the rating was.

Yost: In terms of a project, how large was it? How many programmers worked on it? How long did it take?

Bace: MIDAS, I want to say, a half dozen people worked on it.

Yost: Do you remember what span of years?

Bace: Two to three, maybe. Three usually is a gimmee because three is a (Federal) budget cycle.

Yost: And when was this, exactly?

Bace: This would have been probably 1987-88 time frame was when we probably kick started it. I want to say the MIDAS paper would've been 1989-90 time frame. Seemed like that was just hitting about the time I got into the center.

Yost: It was programmed in LISP?

Bace: That sounds right; would've been right.

Yost: The favored AI language; did that have any . . .

Bace: Oh heavens. Well, people [interrupted]

Yost: . . . implication versus systems programs in other languages?

Bace: I think that their intention was to prototype it as something they might want to consider doing for real. I think also in some ways MIDAS was an example of doing systems to see they teach you. I think it was extremely instructive to a lot of folks inside the fences.

Yost: Can you compare and contrast MIDAS and IDES?

Bace: I think IDES was looking at a more commercial, more of a vanilla commercial platform (UNIX vs MULTICS). But I think also IDES had; I mean, IDES was put out

without any presumption of a resident staff to transition it to use. They assumed that the IDES prototype would be something that they would hand off to someone for commercial development whereas MIDAS was done as an in-house deployment which presumed that somebody was going to actually have to use it and put into production use. To my knowledge I'm not sure that outside of just research and research sorts of applications that IDES ever went into operational use. So far as I know, MIDAS was; at least the last three or four years that DockMaster was actually in production use.

Yost: And MIDAS, it was the first or one of the first token-based I&A?

Bace: MIDAS was strictly an IDS. Any token-based I&A would have been separate from MIDAS.

Yost: Do you recall who led the project with MIDAS and if they would be a good interview candidate?

Bace: I don't know. Of the folks I would choose, it would probably be Eric Shellhouse. I don't know how accessible Eric is, these days.

Yost: Two people I meant to ask about earlier, that we've come across, two early computer security researchers at NSA were Hilda Faust and Dan Edwards. Did you work with them directly?

Bace: No, I did not. The person to ask about both of them is likely Marv Schaefer. Marv should be on your list. So Marv was the original chief scientist, back when it was the DoD center. And Marv's in the area, and I do know how to get in touch with Marv. Marv was in the thick of that; he was one of the founding members of Trusted Information Systems with Steve Walker as well.

Yost: In your book you wrote that after stronger I&As were in external use, MIDAS continued to be used more to detect internal abuse. How big of a problem was that within NSA?

Bace: The need to check for it was always ubiquitous. And the desire to check for it was always ubiquitous. But as part of it, I think that it was just considered a standard of practice, I think, for any agency to handle their security sensitive information assets. You have to have the ability to demonstrate that you've taken due care. It's a due diligence sort of thing.

Yost: You were at NSA roughly a dozen years.

Bace: Yes.

Yost: How did the agency change in that span of time and how did computer security and computer security research within the agency change throughout that span?

Bace: Oh, eons. During that period of time the Computer Security Center itself went through at least two hard restarts where they would back off and rethink how they were approaching things. But also, when I came through the door the mission area actually wasn't INFOSEC, actually, it was COMSEC and COMPUSEC. INFOSEC was about midway through; about the time I went to NCSC. They were dignifying the notion that it was information security now, not communication security and computer security. At the time I was leaving I think they were having to deal with (the fact) that they did not having the luxury of building all these critical computer systems in-house. They were going to have to deal with commercial platforms and the entire organization was still trying to wrap heads around how that was supposed to work. The other dynamic in play was that I came in, in the belly of the curve; of this huge buildup we had in personnel in the 1980s. Bobby Inman, our prior director, had successfully lobbied Congress to pour some bucks into recruiting, and amending pay structures and so forth in order to rebuild after a post-Vietnam War drawdown. I was a beneficiary of that buildup. Lot of the reason is that I applied for the job when it was a dead job market in the early 1980s and NSA was one of the few firms in town that was hiring at all. But also they were hiring folks with my particular skills. As an outcome of that, there were a lot of new employees all at once and they were working with skills better fitted to working with political and financial realities of draw downs. Culture shock, to say the least. Even by the time I was leaving, everybody was saying "okay, we've got to get more efficient about how we're dealing with certain aspects of our mission and we've got to be thinking ahead a little bit more aggressively. But also we've got to think about our expectations; how much control we have over operational environments." So it was a different scene. This was as well; I

came out as the Web was becoming a reality and as the whole dotcom boom was starting. Seeing all this explosive growth, also put a competitive pressure on retaining the personnel. So it was a very, very interesting tumultuous time when I left.

Yost: And did the advent of the Web have a—besides recruiting—have a major impact on NSA before you left?

Bace: Oh heavens yes. It was that entire populations of people you would never ever have thought would go online were suddenly there. But the commercial activity that came with the web also introduced a powerful motivation for adversaries to be there, as well. You had to deal with an adversarial population, with a threat population who were there for a lot broader spectrum of purposes. The issues across the board is this: it's one thing to deal with an environment where your primary adversary is only going to be there to surveil you or to mess with you. It's another [matter] entirely, where they could be there for any of a dozen reasons, all of them obnoxious. Perhaps not all of them critical to you, but of similar import to you so you end up having to do a rack and stack of the prioritization of those threats. It makes things extremely painful; yes, it complicates matters quite a bit. The necessity of dealing with these threats creates markets, which is great for me. (Laughs.) But if you're in the position where you worry about such things, it makes life much more complicated.

Yost: When was the Network Audit Director and Intrusion Reporter, or NADIR, developed at Los Alamos and can you describe that system?

Bace: NADIR was; that have was done on a database platform. That would have been done in the late 1980s, early 1990s, as well. I want to say 1989-90.

Yost: And was that funded by Los Alamos? And was there any connection to NSA?

Bace: Yes it was, Los Alamos; and it had no connection to NSA. DOE monitors Los Alamos and is responsible for security auditing them and their internal networks.

Yost: You wrote in your book on Intrusion Detection that NADIR was one of the most successful and durable intrusion detection systems of the 1980s.

Bace: Yes.

Yost: Can you expand upon that? Why was that so?

Bace: It was stable, first; it worked. A lot of other early IDSs would work and crash for various reasons. NADIR was extremely well-designed and in operational usage for a significant period of time. It was successful; I mean, it was a position where it was actually fully-integrated into the operational scheme for protection. And it had all manner of benefit; it had features that hooked everybody; it enjoyed unusually broad support both from folks who were doing work on the operational side as well as the security and regulatory side of the house. And that was unusual for the day; people usually considered

security to be a roaring pain in the rear. And it was actually making life easier for a lot of the folks that used it. So that was good. I think it won a lot of allies, too in that it demonstrated again, additional due diligence of the systems in question, which were all handling pretty critical information.

Yost: And was it a system that was used exclusively within Los Alamos?

Bace: Yes, it was.

Yost: To what extent were systems diffused to other organizations within government? And if that wasn't occurring, was it because of who funded it, a Not-Invented-Here type of mentality, or what was at play?

Bace: I think at that point people were just getting their heads wrapped around the notion of having distributed systems. Another factor is that there you had a lot more emphasis on local control of systems, and those systems were a lot more often designed for a specific purpose. The notion of having interoperation amongst platforms was not as commonplace as it is now.

Yost: Was publication and sharing ideas within the community prevalent, or were insights kept within groups?

Bace: I think there was a fair amount of sharing, at least across the security community in general. At that point; there weren't that many people working the issues of security, particular outside the fences. But there were two places to be, as a security researcher, at that point in time: you would show up in Oakland in May for the IEEE Conference, and you would show up in DC in October for the National Computer Security Conference. You'd have offshoots of that, depending on what specialty areas you were in. If you were a cryppie you'd go to CRYPTO; if you were a UNIX person, you might go to the USENIX Security Symposium. Another gathering was ACSAC, the Computer Security Applications Conference. There weren't that many security venues and when folks would publish, the publications rear their head at one or the other of those locations. I can still remember doing Oakland at a point where everyone fit very—and it was pretty much everybody who was doing anything of interest in security—fit quite neatly into one ballroom at the Claremont. I can remember the same for the National Computer Security Conference, at the Renaissance at Woodley Park; and there'd be basically one room. The joke was that I'd create a riot because everybody was dressed similarly – except me (laughs) but if they were anybody doing anything of interest in security, you could almost count on them being there.

Yost: And was it fairly easy and straightforward to get clearance to be able to present research that was done at NSA or for DoD at these conferences or was it difficult?

Bace: From what I saw, it was; it varied widely depending on the nature of the work, who was doing the work, who was leading the work, whether it was a contractor or an in-

house person. And I think that people tended to be pretty conservative about their attempts to publicize what they were doing, as well. People seemed to come to some consensus pretty easily of what should not exit the walls versus what could.

Yost: Was it more restrictive for contractors?

Bace: Actually not. I think it was the other way around because typically, I think contractors usually drew on what they knew of the outside world, and limited their discussions to how the outside world interacted with security, in particular what the hardware and software vendors were doing in the area; what the platform vendors were doing. Typically, those are the sorts of things that come into consideration when you consider whether something can pass the classification test.

Yost: Kathleen Jackson was the PI on the NADIR project.

Bace: Yes, indeed.

Yost: Would she be a good candidate for us to interview for this project?

Bace: Yes, if you can locate here. She's not stayed particularly well connected to the rest of the community. Last I heard from her she was in Silver City, New Mexico, I think, in southern New Mexico.

Yost: Wisdom and Sense was also developed at Los Alamos in partnership with Oak Ridge National Laboratory.

Bace: Right.

Yost: Was this the first intrusion detection system to derive its own rule set from audit archives, do you know?

Bace: I don't really know. I want to say that it was; that they were the first vetting-based system.

Yost: And what was the significance of this, can you characterize it?

Bace: I think that people had always been plagued with the notion that; I mean, they again, went back to the Zero Day Attack scene. There were folks of different camps, you know, in terms of thinking about what you should worry about as a computer security person; whether you should be worrying most about the person who's sophisticated enough to know the system better than you did, who would come up with a totally novel new way of nailing the system vs someone using a textbook attack. And it varied very widely depending on folks' attitudes about the strength of the system and so forth. Wisdom and Sense attempted to address perceived deficiencies in what we monitored within systems and how we specified attack signatures as reflected in those monitoring results. There was some criticism in that there were certain folks who believed that the

Wisdom and Sense approach was simply a solution looking for a problem to solve. Gunar Liepins, who was the lead from Oak Ridge was a total technology water walker, in particular, he was expert in the areas of genetic algorithms; self-healing and the learning system arena. I thought that he and Hank Vacarro had some real interesting results. The implementation would drive us crazy from time to time; with issues of stability and scalability; and actually learning to use the system was a challenge. We never really got it to a point where we could test it against anything resembling a large system - Gunnar killed himself shortly before they ceased funding the project at the end of a program cycle. His demise was a shock to me and the rest of the research community. It was really interesting work. And I think Hank Vaccaro took some of the things that they developed into the commercial realm in other application venues

Yost: The Distributive Intrusion Detection System (DIDS), which you brought up earlier, was funded by the Air Force, how did that system come about?

Bace: I think that DIDS was an unusually rich collaboration; Tim Grance, head of a research group for the Air Force had successfully hired a real interesting set of talent into his team at Air Force. They were out of the Air Force cryptologic command. And they had distinct ideas on how one should address dealing with a distributed system, with monitoring; sort of expanding the vision of intrusion detection, which up until then had been pretty much single host-based. And I think that Karl Levitt and Biswanath Mukherjee at U.C. Davis had similar ideas. There were some amendments and some variations from the original designs of intrusion detection that needed to occur and we

had an appropriate stable of graduate students to work the problem. The entire DIDS project was fascinating. It was a lot of fun; extremely educational. A lot of; there again, the tech transfer from DIDS was immense. Deb Frincke, who's at NSA now, came out of that project; Jim Alves-Fosssis at the University of Idaho came out of that project. Chris Wee director of security architecture for Juniper and did five or six startups before that; did his Ph.D. dissertation work out of that project. Just an incredible body of folks; probably a dozen different folks did dissertation and thesis work out of this, who are all still actively working in various security-related functions in the industry.

Yost: In terms of the technology itself, were there government developed systems that were deployed in the commercial sector?

Bace: I think that the system design ended up reflected in the first generation of commercial systems. And actually the core Air Force group along with some folks from, Trident Systems formed the Wheel Group, which did Net Ranger, an early successful NIDS, which was then acquired by Cisco. The core AF team comprised Cisco's security team for well over a decade and some still lead Cisco's network-based security product efforts. Yes, we got our money's worth out of that investment, in terms of product/concept tech transfer – and people tech transfer as well. When people leave these sorts of projects, particularly if they happen in the educational realm, they take the intellectual foundation—the way the problem is approached and the solution designed—with them, typically. Their work is influenced by these experiences - they comprise the

basis on which they build and evolve their subsequent solutions—and this was no exception—at UC Davis.

Yost: So DIDS, in many respects, is the origin of many of Cisco's

Bace: Right. DIDS likely colored anything you saw for quite some time in the network intrusion detection realm for Cisco.

Yost: In the early 1990s some commercial products hit the market. ITT ComputerWatch; can you describe the commercial environment at that time and what impact ComputerWatch or any kind of research appropriations and ISOA?

Bace: This era marked the point at which folks understood that they had something of value in IDS. They did not really have what ought to be their marketing approach nailed down very well. This was a matter of the geek vs business person conflict; I mean, Tom Berson, whom I consider the token business person for the security realm, having been there before with his original startups that he successfully exited would say, "you know the difference between a geek and a businessman is that a geek goes off, designs something fabulous and wonderfully technologically clever, and he goes out and he makes people buy it. On the other hand, the business person comes in and says "let's talk about your problems" and then goes out and builds a product to help cure them. I think that a lot of that first generation of products suffered from that dissociating with the difference in mission between geek and businessperson. (Laughs.) But there were some

as I recall, like Computer Watch, that did sell a respectable number of units. There were widely varying clarities of vision in those early products. And also, there was a lot of variation in people's understanding of what represented an optimal solution to the security problems. There was a lot of kind of snake oil salesmanship that went on in those days. But you see a lot of such problems in any early technology market. I mean, the other disconnect I saw was that you would have folks that were coming in as hard technologists, and in some cases, hard technologists just don't do appropriate engineering analyses of problems. So they would devote a whole lot of the limited resources of the system to looking for a particular problem that was extremely remote or rare (though interesting!), when they had a Mack truck-sized problem next to them that they would totally ignore. (Laughs.) I used to think "oh my goodness, we're just being incompetent," until a couple of friends in the startup realm in Silicon Valley buttonholed me and said "hey, this is just the way these guys think"; "this thing is just a really typical evolutionary path that pretty much all new technology goes through. You're going to have these disconnects and the market will be all too happy to correct them over time. Be patient. Let it go through a couple of product cycles and then the market will weed them; it will weed the ones that don't pass muster awful quickly."

Yost: As users, what industry or industries were early adopters of intrusion detection?

Bace: Trying to remember. Part of me wants to say financials, for sure. And there were certain folks in the financial community who were much more aggressive than others.

Yost: Are there certain corporations that stand out?

Bace: Well, the joke we've always had is if you're trying to do something bleeding edge, that you wanted to have a particular information risk executive at a major Wall Street Bank as your champion. So Wall Street would be one of the regulars. Some folks within various aspects of the intelligence community could be good allies. Some of the —that's varied really widely— some of the telecom carriers could be good allies, as well. But it became kind of dependent on the resident person in charge—sticky (i.e., long-tenured), visionary, whatever—was. So you'd have certain players in the market who demonstrated, and word got around fast, that they were capable of understanding what you had to offer and why they should buy it. But the right folks also, had enough collateral internally and politically to expend on budget and so forth, so they'd get their way. You had certain folks who were better customers than others but the joke is "the usual suspects" that you could count on to at least be approachable if you had a new solution in mind.

Yost: And with these customers, can you discuss kind of the economic tradeoffs; the costs of running intrusion detection systems, as well as purchasing them? Is it fundamentally a challenge to convince them of the risk or to assume the new costs for something that they haven't spent money on before?

Bace: The area of intrusion detection was unique and I argued that it was critical to security in general. That's one reason I put so much energy into it. I felt that it was

critical to the rest of security management technology in that if you did not have the evidence that the attacks were taking place there's no way that they would be visible to you otherwise, [and] your chances of building out anything resembling a security program were probably going to be nil. You needed evidence that you had a problem and intrusion detection was uniquely positioned to provide that evidence dead to rights.

Yost: Very strong argument that this is the place to start.

Bace: Indeed. And I think that the folks who were the early adopters got that and subsequently were strong champions. But I also assert that they were winners from it as well. They were usually the folks who would build empires on this.

Yost: It was 1996 that you moved from NSA to Los Alamos?

Bace: Yes.

Yost: Can you discuss that change.

Bace: I was in a position where I just needed to get out of NSA. My son died in 1994 and I was going through just a difficult time; ironically, the intrusion detection stuff was starting to move forward, starting to get a lot of attention, getting a lot of political currency and it was a fabulous place to be but it was also a horrible place to be, politically. I, paradoxically, was not highly positioned enough in the opinion of some of

the management, even though I had successfully built the program, to run it at that point. (Laughs.) And I also just needed, in terms of recovering from the loss of my son, I just needed to be somewhere different and the folks at Los Alamos offered me an opportunity to come there and to basically get a different exposure, geographically as well as functionally and corporately. And they thought that being in more of a predominantly research organization might be a better fit for me. So I went to Los Alamos. In some ways it was lovely and in other ways it was totally horrible. I finally got real about the fact that I am not a good bureaucrat. (Laughs.) Particularly working security venues; in any sort of a nuke lab setting is an inherently extremely bureaucratic endeavor. Also, I had a lot of physical problems that came from the altitude. So between the two, I decided pretty quickly that I needed to be elsewhere.

Yost: What was your position there, and what types of things did you work on?

Bace: I came in as Deputy Security Officer for the Computing Division, with the understanding that I would ascend to being Security Office for the Computing Division within a year's time or so. I was overseeing a nontrivial security staff with the most incredibly extensive regulatory requirements I could ever imagine. I mean, there were literally rooms of security policy documents and we had to be in compliance with all of them all of the time. But also, there was an immensely complex computing end of it, both in terms of the range of platforms, we covered everything from the gray class supercomputers down to the bleeding edge, you know, computer on a chip; a monitor on a chip sort of deal. But also, it was a different game from NSA; a lot more edgy, bleeding

edge computing research; a much more expansive set of research topics, as well. Los Alamos was charged with being the stewards of the nuclear stockpile. It's not, as most people think, it's not the place where the weapons are designed or produced. Those are all other labs, other peoples' venues. That was the irony of the Wen Ho Lee case, I thought, in that this was not the mission of Los Alamos. Los Alamos was charged with dealing with the impact of an aging nuclear infrastructure – for example, having to deal with the environmental impact and how one gracefully phased used fuels and used weapons out of production. But they also dealt with other sorts of nuts and bolts of dealing with the nuclear realm; and the expansive medical nuclear domain, where they would deal with disposal of radioactive medical waste and things like that. So it was a fascinating place to be. I think it was the most highly educated community in the world, in terms of the density of Ph.D.s and so forth. And it's actually, within a lovely, really tight little community; maybe 30,000 people there, all located within two primary small town sorts of settings. And it's just a gorgeous setting, all told, and very remote, and a seriously high mountain, both physically and bureaucratically. (Laughs.)

Yost: And can you characterize the computer security research with Los Alamos?

Bace: I'd been sitting in on teams doing a lot of extremely innovative work. Just fabulous. Another person [with reason to be] on your list is a guy named Gary Christoph. Gary came from Los Alamos; Gary actually is the person who recruited me to Los Alamos; he was Chief Security Officer and stepped down shortly before I got there. Gary is Ph.D. is physical chemistry, Cal Tech alumnus, and he had, at that point, been working

on using a variety of advanced analytics on computer audit trails and transaction logs for purposes of fraud detection. And they, at that point, were working for HCFA, the parent organization for Medicare and had successfully used their techniques to spot major instances of Medicare fraud. In particular, one fella in south Florida had taken them for something like $35 million worth of adult diapers. It was just totally amazing work (and results). Anyhow, Gary's group was doing a lot of innovative things in fraud detection, looking at computer-based evidence. And there were other researchers who were doing similar things along those lines. It was just a very idea rich group, and you would have folks who would do amazing, amazing work. There was one guy who was researching forest fire risk - he was able to reliably reflect where lightning strikes were imminent, subsequent forest fires were likely to hit, and what sort of damage they were going to do using Monte Carlo simulations with statistics. So you'd have these sorts of folks and that caliber of mind working all over the place. There was just no telling; I never knew what I was going to find when I went to work every day.

Yost: Sounds like a fascinating place to be.

Bace: Oh yes, very much. I'm a sucker for these settings. (Laughs.)

Yost: I understand that you were involved with helping to detect or identify an attack by computer criminal Kevin Mitnick. Can you talk about that?

Bace: (Laughs heartily.) Oh, I would say I was probably at arm's length with that one. I had a linkage, a friendship, actually a long term friendship, with Tsutomu Shimomura, who was at the time at the University of California San Diego, out of the supercomputing organization there. Actually, when I originally met Tsutomu; he was an adjunct at Los Alamos and—totally fascinating—if ever there were a savant, you know, who could look at a piece of technology and say you need to worry about this, this, and this, he's it. Classic case of what my redneck relatives would label "second sight." Fascinating guy. He was always good for instigating interesting ideas. He was totally fascinated by the idea that you could actually work on computer security and people would actually pay you to do it. So we had a long-standing, ongoing conversation, in which we would periodically figure out whether there was a research topic we could nail down and he could work for me. Never could quite nail that down but it became an excellent excuse to spend time at San Diego when my travels brought me there. Also, when I'd run into a brick wall trying to figure something out, he'd be a good go-to guy I could call. So anyhow, one of the things the IDS research community decided to do is in order to move forward a little bit more briskly with intrusion detection technology so that we could do buildable products, is to take a fresh look at how you overcame problems that were persistent, because we'd always run up to the same roadblocks over and over and over again. So I sat down with the other folks who had funding authority within the venue and we said "what if we actually arranged or orchestrated a set of meetings with people and we invited people who were gurus; they were four-star, best experts in the various areas; in those areas that always present perpetual roadblocks for us." And what if we put forth the challenge; telling them what we're trying to do, and getting them to come in and give

us kind of a graduate level fast track acquaintance with their areas of expertise and how they might relate to what we're trying to do. And finally, what if we then asked them for their best shot, knowing what they know about their problem area, of how they would, if they were in our shoes, apply what they're doing to our problem." So we set this up, kind of tongue-in-cheek—called it the Guru Conference —and Tsutomu was one of the folks we invited. Well, we had a couple that were relatively uneventful. I think we invited Gene Spafford to the first of them; he decided to stay for the rest of them and joined the IDS research community as well. (Laughs.) This was when we started funding IDS research under the auspices of the COAST project, precursor to Purdue's CERIAS. But the third time we threw a Guru Conference, we had the culmination of our original design; the original vision called for us doing this in a really sucky weather period—which is January in DC—we'd go to California; we'd go somewhere really nice so that the brightest people would be more inclined to come; and we would leverage these factors to make sure we had all the right people around the table. Well, the first two years were okay; you know, we had hits and misses. However, the third year is when it all came together, in January 1995. In January of 1995, I was arguing with Tsutomu about one thing or another and it turned out that was the year that the Sonoma Mission Inn actually called us said "if you want this week in January we'll give it to you at this price" and it was our first time we could afford it under our budget. We said okay. This is January, like the third week in January, Sonoma Mission Inn, okay this works; enough hot tubs to satisfy everybody. This will be a fetching enough proposition so we think everybody that we invite to come to this one will probably come. We hit all of our goals - the gurus that we wanted were available for that week; they were like, "hell yes, I'll be

there." Then the week of the conference, Mission Sonoma, and that area of California, has a 100-year flood that starts a day and a half before we're supposed to start. So about half the attendees get flooded out, or stranded on the far side of the Russian River from us. A fair number of others had come in early; I had set out early; I had flown into San Francisco a day earlier, and then Kathleen Jackson had flown in from Los Alamos, and then Ruth Nelson, another of my "No-beard" (i.e., woman pioneers in security) friends, had flown in from Boston. So we had all converged on San Francisco and decided to drive up really, really early the day the rain was supposed to start; were willing to come in early to get things going. We got there okay, driving through flooded roads as we got close to Sonoma. Later in the day we had people who flooded, you know, who washed off the road. It was just totally nuts— some folks ended up coming in at three o'clock in the morning. But we all got there and it turns out the other two groups that the Mission Inn had booked had cancelled out because of the flood. I was getting phone calls from folks on the far side of the river. By morning, the river went down and they all showed up; so we had Mission Inn to ourselves. Tsutomu showed up at the last minute —after a set of rather tense conversations with me - shows up the girlfriend of a notorious cyberpunk on his arm and an ice axe, having come in from the ski slopes in Tahoe. I said "if you're here, you better damn well be prepared to present something interesting." He said "well, I have something you might find mildly entertaining," and he proceeds to get up and present to the group as a whole. The presentation he had was of his Christmas Day intrusion and the system that he and Andrew Gross, (who was a Ph.D. candidate who worked with him at the UCSD Supercomputing Center) had pulled together to monitor his system at UCSD. And he described how they had started their trace back activity

using the monitoring system results; and everybody in the room was totally fascinated. We had all the right people there to discuss what was going on with regard to the intrusion. And everybody was saying "oh, well if you do it this way versus that way, it would be a lot more provable. You need to be talking to this person versus that person." So I was thinking "well, that's interesting." So he calls me, I guess, the following Monday, on my way to the office, and says ah, you may want to stop by, you may want to swing by a 7-11 and pick up a newspaper; there may be something you may find a little interesting. So I pick up a New York Times newspaper; lift the fold to find the top left article covers report of the intrusion complete with allusions to the Guru Conference. I'm thinking "well, this is interesting." So from that, a fellow from the North Bay Area called the reporter at the New York Times ; and said, "well actually, I have a file that showed up in my comments space that I stumbled across that appears to be some of the stuff that is reported here as having been taken. Maybe I should contact this guy and tell him about it." The reporter calls up Tsutomu and lo and behold, the guy had it. But the guy had also had the audit logs for the intrusion into his system and they were able to use them as a means of tracing back. At that point, everybody was involved in the trace back, I think, in that research community; aside from us who were statutorily prohibited from doing so. And this goes on and I'm thinking okay, "this will be intellectually interesting, if nothing else, at least in documenting how you might do this trace back, you know, if it's feasible." So Tsutomu calls me, another of those days you could only dream of—I had bone surgery, dental surgery, on my jawbone; so my face was swollen out to here and I was sedated—and the phone rings at 11:00 p.m. My husband answers the phone and he says "well, she's out of it." Tsutomu says, "relay her this message, 'you may want to stop

by the 7-11 on your way to work and pick up a copy of the *New York Times* in the morning. Clue: Scott Charney is in a press conference right now talking about the matter we've been working on.'" And I'm thinking, "holy shit! What on earth is going on?" We get up in the morning, we stop by 7-11, and because we're in a hurry, I just tuck the paper into my purse to read when I get to the office. I walk into my office and I have one of the other technology teams who are basically a bunch of kind of ex-army sorts of commandos who are doing a fairy ring dance around my desk. They asked "Have you read the paper yet?" I said "the paper's right here" "Why are you asking?" "Because Tsutomu caught Kevin Mitnick." (Laughter.) I'm thinking "well, this is interesting." But it was a fascinating time; totally fascinating time. So a lot of good came of this in the pure research sense - Andrew Gross went back and did basically a second dissertation and in it talked about the advances he made in investigative technology. He had actually made some quantum strides in how you decompile a disk image for certain platforms. The monitoring platform he'd designed and was using was also apparently considered groundbreaking. But he also did a second part of his dissertation on how to do network tracebacks and replays. So we got useable research out of the investigation as well; publishable research. But it was still not a development I was prepared to deal with. It's certainly not one you'd expect from inside the intelligence community. But Tsutomu is a great deal of fun.

Yost: Had you been involved in trace back work for NSA?

Bace: No. There, you're interested in how one collects an audit trail, and what comprises artifacts, and what allows it. On the one hand, I'd always been fascinated with the confluence of law enforcement and how one does, effectively, the forensics of a network intrusion. That question has always been fascinating, because that, to me, that's instrumental to the value of an intrusion detection engine; it's one of the things that people assume that an IDS will give you by way of capabilities. That the assumption was that an IDS and an audit system, would give you the ability to do forensics when you need it. But conducting tracebacks is one operation that I didn't ever do, hands-on. [In] fact, we consider that to be a fundamental ethical issue.

Yost: Did you start Infidel, Inc. right after working at Los Alamos?

Bace: I took a short stand at EG&G, and it turned out that I'd been hired into a spot that had been programmed out because during re-org someone just forgot to tell the folks who had hired me that they were being downsized. (Laughs.) So I did an extremely short stint there; and then was coming back to Maryland and was in discussions, actually, with another federal agency to come back to work in DC. In between I got a call from a dear and old friend who was director of fed operations for Cylink. It was sort of the only commercial firm in existence at that point in security. Cylink did the point to point link encryptors used by most of the financial institutions in the community. And Cylink was going through a major rethink of what they wanted to do, going forward (they were having the same COMSEC to INFOSEC crisis as NSA) and wanted somebody to help them as they considered building out an acquisition program for more computer security

startups. So they engaged me for a consulting gig, which landed me in the middle of Silicon Valley, just as the dotcom boom is becoming real. And it was the ultimate intellectual candy store; just a fascinating place to be. So I spent several months at Cylink and I decided "oh hell, I like doing this; I like the ability to flex to the task at hand; and there are plenty of tasks to work." So, I ended up, through Marvin Schaefer, who introduced us, meeting Terri [Gilbert], one of his childhood friends, a veteran of the Valley. And Terri had a spare bedroom - a place for me to perch that left me less victim to the hotel room scene in the middle of the dotcom boom, which was pretty treacherous at times. (Laughs.) But she also had done a dozen or so startups of her own, so kind of knew that venue well. So I said "alright, why don't we just set up business together" and see what happens. So we incorporated Infidel and set up practice together, and away we went. Kind of marched on from there.

Yost: So basically, a lot of your consulting work was out in Silicon Valley?

Bace: I mentored, advised, and did consulting gigs with quite a few of the startups in the security market, and ultimately ended up in cahoots with Trident Capital, doing the tech side of the venture capital scene, so it was a lot of fun. In the early days I advised a group called IntruVert, who were acquired by McAfee and formed sort of the crux of McAfee's business. [I] advised Security Focus, which was acquired by Symantec. At one point, I think I was on advisory boards of a half dozen different firms. And then at Trident, funded Qualys, who will go public later this year, depending on the market. [Went public in Sept. 2012].

Yost: having an investment strategy…

Bace: Qualys is solvent. It's been maintaining a really sweet growth rate; but also it's profitable so I think those will work to our advantage. Trident was a great place, as well. They did about 13 security-related investments and so far, I haven't lost one. I think we're up to seven exits now so it's cool. It's worked out nicely. We've got something that materially changed the face of the security market, as well, and I like that. I had a hat trick; three exits that closed within a month and a half of each other, which was great fun. (Sygate which was acquired by Symantec, and forms sort of the crux of their endpoint security strategy, Tablus, in the web security area which went to RSA and Thor Technologies in the area of secure provisioning which was acquired by Oracle.) Several other firms in in the portfolio exited in the meantime. We did TriCipher in the identification authentification space; it was acquired by VMware. We have a couple more that I think are going to do very, very well that are still growing. I've got HyTrust in the virtual machine security management space. That was just sweet; it's the easiest investment we did in the whole time I was at Trident. Trident continues to do some security investments, but these tend to be a lot more infrastructure-centric. And when the financial crisis of 2008 cooled off the investment space, I got an offer to come back east. I had always vowed to myself that I would come back east and do a little more government stuff, leveraging what I'd learned in the Valley. So I came back and went to InQTel for a year. And I worked on cyber security investments there; and at the end of the year I decided that I was still bureaucratically challenged, so I left. I went through a

health crisis or two, which got me thinking in real terms about bucket lists; and I just took a post—I started recently—with University of South Alabama, starting an applied research center [which] hopefully will focus on forensics. A few pet peeves of mine; and one of the pet peeves is we still don't have a consensus for an Underwriter Labs sort of realm for computer technology, in general. We need to have a situation where if somebody makes an allegation about the capabilities around a piece of software, or hardware, or an integrated system they've got a place to go to ascertain what it does and does not do, and can rest assured the analysis has been done to some degree of rigor.

Yost: So you've scaled back your Infidel consulting?

Bace: I do a little bit of advisory stuff on the side for Infidel, but in general, Infidel is a low level activity right now.

Yost: Are there any areas that I haven't touched on, questions I haven't asked that you feel are important to understanding your history and the history of intrusion detection in its early years?

Bace: No, none that I can think of. There were some very interesting times. Although one area that I think we haven't talked about is that I did help and try to pull together a set of community supports for the FBI, when they first spun off their security group. And I still think there's a fundamental culture clash there between the way the FBI typically approached how you investigate crime and some of the variations of it that need to occur

in order to deal with the computer aspects and the computer security aspects of that. So I dealt with Jim Settle, who was the lead of the first squad working computer crime. It was fun; it was very, very interesting. I was mentoring his initial squad, because you had folks who may have had raw exposure to technology or to law enforcement, but they were pretty much coming at the whole security thing cold because they really didn't have any particular preparation to understand hacking, or how to recognize a hack, and how you might have dealt with a hacking incident. And there was a lot of fuzziness surrounding the mission of the squad; the tasking they got for the caseloads. So I've watched that area with great interest because that's been a seriously arduous area; that convergence of the law with security. I joined forces with the coauthor of my second book, "*Forensic Testimony*," when Fred Smith was a deputy attorney general for special crimes for New Mexico - he served in the capacity for several terms. And [I] have always been sort of a free thinker about that overlay of technology and the law, so I suspect I'll continue to be active in that realm.

Yost: I assume you've been an expert witness many times.

Bace: Oh yes. It's always a great deal of fun. It's like hacking, it's a lot more fun if you understand the system before you get there, as opposed to coming at it cold. There've been a couple of times where the judges get tickled because it's obvious I understand the bigger game better than the person who's attempting to cross examine me. (Laughs.) It usually creates a fair amount of entertainment. But I've also looked at a few of the intellectual property disputes, as well, that have seemed to have proliferated in the

security realm; some of the arguments there are just eye-rolling. But it's fun; you get an appreciation for why attorneys get the bucks they get. I used to wonder about what on earth I was doing in engineering, because I thought that engineering was a pretty dry and linear and, you know, very structured sort of discipline and I am not that type of person. But it turns out probably that system engineering is the only thing that would've prepared me for doing anything I've ever done (in security) because it's just all a part of the bigger system. And in any system the most interesting place to perch is across the system junctures, and security resides atop the juncture of all of it. That works nicely. Anything else here?

Yost: No. Thank you so much, this has been really helpful.

Bace: Oh, this is great. It's a fun domain. I think you'll have an entertaining time with some of these characters.