An Interview with

EUGENE H. SPAFFORD

OH 430

Conducted by Jeffrey R. Yost

on

12 November 2013

Computer Security History Project

Purdue University, Lafayette, Indiana

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

Eugene H. Spafford Interview

12 November 2013

Oral History 430

Abstract

This interview with computer security pioneer Eugene Spafford spans from his early education to the near present (2013). He discusses how he came to focus on computer security as a research field and his long and ongoing career as a faculty member, editor-in-chief (*Computers & Security*), center director, and educator. A substantial portion of the interview addresses his work in founding and leading a premier center for computer security research—COAST Lab (Computer Operations, Audit, and Security Technology*)*, which evolved to become CERIAS (Center for Education and Research in Information Assurance and Security). CERIAS is the largest academic research center on information assurance and computer security and has had tremendous influence on the field from its pioneer research and education to its highly regarded symposiums and outreach. Among other topics Spafford discusses are intrusion detection research and development, Unix security, Tripwire, the Association for Computing Machinery, service to the federal government, and the importance of a sense of humor.

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. I'm here this morning on November 12, 2013 with Eugene Spafford. This interview is for CBI's NSF-funded project *Building an Infrastructure for Computer Security History*. Can you begin by just answering some basic biographical questions that tell me when and where you were born?

Spafford: I was born in Rochester, New York, on March 26, 1956.

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

Spafford: I was really interested in science and mathematics growing up. I took a lot of science electives. Not in biology, that was not high on my list, but most of the other sciences. I also was a big fan of science fiction. I did a lot of reading outside. I was interested in history, too. So by the time I was done in high school, I had background in a number of different areas and really wasn't sure what I wanted to do.

Yost: You attended SUNY Brockport and majored in math and computer science?

Spafford: It was not a direct path. When I graduated from high school, I had a New York Regents Scholarship and I had applied to several different schools. The one that seemed at the time to be the best choice for a number of reasons, economic reasons primarily because I could live at home, was the University of Rochester so I started there in the fall of 1974 as, I think, a math and physics double major. I was commuting and I was also working part time because the Regents Scholarship didn’t cover all the tuition. So I was working very long hours and was finding it really tough to be able to manage both an almost full time job and school.

I wasn’t doing overly well in the classes. Looking back, it was a rather odd mixture of classes that I signed up for as a freshman – I have long since realized how important course counseling is for undergrads. Also, I didn’t get involved in any on-campus activities because I wasn’t living there, didn’t really know anybody, didn’t have any time to get involved in any of the extracurricular activities.

And then, early in 1975, my father hurt his back and had to take time off work, and eventually lost his job because he wasn’t able to get in to work. My sister was still in high school; she was a junior in high school and so I just made the decision to quit school indefinitely. I withdrew, actually, and went to work full time to try to fill in for my dad being out of work, until my sister finished high school.

So that went along until she graduated in 1976, and one of the schools that she was really interested in was SUNY Brockport because they had recruited her for a time-variable degree program that they had. It was a three-year undergraduate experience, full regular degree. I drove her out to Brockport a couple times to attend some of the informational meetings and sat in on them because she was there. And I got really interested in it and applied, and was accepted into the program. So we both began together in the fall of 1976.

Yost: And did you give any thoughts to what kind of career you wanted while majoring in math and CS?

Spafford: As I recall, I actually had several different fleeting interests at the time. When I was in high school, and then for a little while, I thought maybe medicine. So when I was in high school, I attended classes and got a rating as an EMT. I was the second youngest person in New York State who ever was licensed as an EMT. That experience doing some emergency work, volunteering at the emergency room, the volunteer ambulance corps, convinced me I did *not* want to go into medicine because I couldn't stay dispassionate. I couldn't remove myself well enough from some of the people who had tragic circumstances and someone who just did stupid things, their health problems. So, yes, I knew that wasn't going to be my career.

Law was one that I thought about a little bit for a while. When I started at Brockport, I was interested in physics, chemistry, math, law; I wasn't really sure what I wanted and the program, as I mentioned, was a time-variable program. It had been funded by the Carnegie Endowment Foundation and had been established as a way to merge the liberal arts core in such a way that it was interdisciplinary. All the electives were actually kind of merged, in some way.

One of the first semester courses that I took was environmental science and public policy and computing all rolled into one. I got exposed to some online computing, using simple programs to do environmental simulation, and got very intrigued by it. Found that it was something that, for whatever reason, I was able to do very well. It wasn't my first experience with a computer by any means, but it was the first opportunity I'd had to work in an interactive environment and it really attracted me. So in the spring, I took a computer science course, did extraordinarily well, got highest marks in the class, and by that point I was hooked. So by the time I graduated at the end of three years, I had a double major in math and computer science, and a minor in philosophy.

Yost: Were there any faculty members in CS that were particularly influential to you as an undergrad?

Spafford: Yes, probably the most influential, in some respects, was Dennis Martin, who was my undergraduate advisor for computing. To this day, I still correspond with him; I'm still in touch with him. Interestingly, I met him before I went to Brockport. His brother-in-law was one of my friends in high school and we shared the same birthday. So I just happened to have met Dennis at some events at my friend's house.

Dennis was involved with the math program and he was also involved with the computing department; the two were closely allied at that time. Several of the faculty there were transitory; they were adjuncts or they were only there for a little while because there was huge demand for trained computer scientists. Dennis stayed and had a big impact on many of us.

My math advisor was Sandy Miller, and he was the second most influential. He taught me graduate-level material in the guise of undergrad math. And Sandy still is there, I think he's the head of the department now. He's a distinguished professor at SUNY, and he's the head of the math department. His wife, Jill, was a research computer scientist at Xerox Labs in Webster, just outside Rochester. She came in to lecture, occasionally, and to teach an operating systems class. She also introduced me to some formal work in cryptography, and that was important. All three had a major influence on what I did, and my decision to go to grad school. All three encouraged me to try to do more than I thought I could.

Yost: Did you decide to go on to graduate school at Georgia Tech immediately after graduating or was there a period in between?

Spafford: Yes, there's a story there. I suppose there's probably a story with most things, and I seem to like to veer off to tell stories.

So throughout my undergraduate career, I had a very serious relationship with a young lady who lived in the area. She was an artist, she was going to art school, and so that's a factor in this story.

Also, as part of the background, I worked in the computing center. I had showed an early facility not only with just programming, but with understanding system operations and, I guess, like many security people, I found ways that the system wasn't properly secured and sometimes used that for practical jokes. They decided that with the aptitude I showed, I should be hired. And I remember the director of the center, who's since passed away, Norm Plyter, was very supportive of students learning outside the classroom so there were several of us that worked in the computing center as students.

During the last half of my second year, as I recall, the college got a brand new minicomputer made by PR1ME Computer Corporation, outside Boston. I don't remember the exact city. But PR1ME was a fairly advanced minicomputer for the time that was based on architecture that came out of Honeywell; it was derived from some of their secure architecture. And it was a fascinating machine; still to this day, looking back, it had unusual memory architecture, a protection architecture that was inspired some by Multics. It was really a very nice machine and I got to know the internals and how to program the machine very well.

When it came time for me to graduate the folks at PR1ME Computer who were in the regional office said that because of what they'd seen me do, they'd be very interested in employing me. But they had a temporary hiring freeze on and suggested I go get a master's degree to be more employable, and they'd offer me a senior position. So on balance at the time, I was thinking alright, I'll go. My girlfriend has got another year of school; I'll go for a year or maybe two to get a master's and she can join me. We can get married and I'll have this job outside Boston, and I've always liked Boston so I thought that would be a great match.

So I sent off applications to several schools. Georgia Tech responded with enthusiasm, both because of my academic record, which was very, very good — I had won the Outstanding Senior at the time of graduation — I was actually asked to give the address at the graduation ceremony for the college — but, additionally, I had shown on my application that I had experience with PR1ME computers and they had just obtained three top-of-the-line ones that were there for a research project that was going on. So they offered me a full fellowship to go to Georgia Tech for the first year. It was a little further away than what I had planned on, but the price was right and it looked like an interesting environment; great school, reputation-wise.

Yost: Was this for just a master's? You hadn't thought about a Ph.D. at that point?

Spafford: I had indicated master's or a Ph.D. and I was still thinking master's. So I went to Georgia Tech and the situation changed. During the first year, in March, my long-time girlfriend decided that no, when she graduated she wasn't interested in joining me, she was going in a different direction, and we broke up; well, she dumped me. That was a little traumatic at the time.

The master's program was two years, basically, so I had to go back for the second year, and was offered an assistantship for the second year because the fellowship was only good for the first year. The second year, they gave me a research project that was involved with designing some new algorithms optimized for the underlying hardware. There was one other person there that was really, really into the machine as well, and I was learning from him and teaching him as well some things that I learned. So I did my master's thesis work there.

And on the master's thesis, the timing was such — they lost a number of faculty about that time and they didn't quite have enough to offer all the courses they wanted — I was given the opportunity to design and teach a research class in architecture and OS in my second year as a grad student. That was related to the operating system I was building for my master's thesis. And I loved it. The combination of doing the research work and designing and teaching the class was just so attractive to me that I decided that yes indeed, I did want to go further if I could afford it.

Yost: Is this the Clouds operating system?

Spafford: Not yet. This was just a teaching operating system that I had built to demonstrate memory behavior under severe load.

The faculty there encouraged me to submit an application to the NSF for a graduate fellowship, which I did, and I received one in the spring. I took that as a sign to continue, and so I ended up staying at Georgia Tech and completing my Ph.D.

I taught another couple courses even though I didn’t need to — I had the fellowship. That was good and bad, in that the fellowship gave me a certain freedom but it also meant I didn’t have to pick a thesis project right away to work on something. So I spent a lot of time, I’ll say, screwing around. I actually was doing interesting things but not things that were making progress towards graduation. I think I ended up taking every class offered by the department except for two. And that has served me well in the years since, but was quite unusual.

The Ph.D. at the time required doing a minor sequence, and so I started in psychology. Of the five-course sequence, I think I was in the fourth course, near the end, when I got into an argument with a professor who was a very old-school behavioral psychologist who believed that there was no such thing as free will, there was only conditioned response behavior. This did not sit well with me at all and he strongly encouraged me to drop the course, implying that if I did not, the final grade would not be good for me as a graduate student. But he was the only one who taught that course and it was required for me to complete the minor sequence so I dropped it and had to do a different minor. The new minor was in operations research.

With all of that, I did a lot of course work, used up my NSF fellowship, and did RA work on a couple projects. Eventually landing in a project, and getting support from Rich

DeMillo who was doing work in software engineering at the time, and he had formed a software engineering research center at Georgia Tech. So I was there providing support and learning about software engineering with him. He had funding from a couple projects. I'm trying to remember what year, I think it was 1984. Actually, I think there had been a government shutdown that occurred. I think it was 1984, the first one with Newt Gingrich and crew in Congress; and so the money that he had was frozen and he wasn't in a place to support me. I actually spent a semester working for the Army Information Research Lab that was there on campus. Then I went back, finished my degree, in 1985; no, excuse me, early 1986, and went to work for Rich as a post doc. I got married in the interim. My wife was in a training class for getting a securities agent's license, so we wanted to stay in the Atlanta area for another year, so I took the post doc position with Rich.

Another thing that's notable about my grad career there is I graduated with basically an advisor on paper only, and never published a paper on my dissertation work. I had been doing work on building the distributed kernel for the Clouds operating system, which was a group project that had been funded by various agencies. The advisor who I had started with and who I had done the proposal with left Georgia Tech and went for a year to Carnegie Mellon and then left for industry. Somewhat of a volatile individual at the time, he at one point decided that he was just going to drop all ties to Georgia Tech, including his students, so I was left somewhat adrift with two-thirds, three-quarters of the kernel of the operating system written. I was being supported financially by Rich DeMillo, who wasn't even involved with the project but I had to work on his projects too.

Yost: And was this kernel focused on security of the operating system or not?

Spafford: Security was part of it. It was really distributed systems, it was fault tolerant distributed systems, so that if a system for any reason stopped working the data would not be harmed. It would be recoverable and this involved using what are known as nested atomic transactions, all or nothing transactions. There was a lot of theory that went into this, and design. So I built an underlying system that was supposed to be used for experimentation and demonstration.

When my advisor left, the group and the department head decided that I had probably done enough and been there long enough that I certainly deserved the degree. So they got two other faculty, including one who had just arrived, who was a brand new assistant professor, to be — on paper — my advisors. And I didn't get a lot of advice; I didn't get very much advice at all. But I finished building the system, did the write-up, which looking back, I'm rather embarrassed by that write-up. Nonetheless, it was sufficient that they gave me the degree in 1986, but I never got any publication out of it because I didn't have that guidance. I didn't have that faculty member who was really involved to show me the way. And back then, it wasn't so much the norm to do a lot of publications as a grad student. So that was kind of the end of that.

Yost: So you worked as a post doc for the software engineering group. Can you talk a bit about what projects you were focused on in that year and a half?

Spafford: Part of what I was doing was helping supervise half a dozen students who were involved on projects. Much of what was going on in the center was testing-oriented in one way or another.

The first project I got involved in, I was looking at the comparison of some tests — I need to back up a little bit on this. I'll tell you a fun story that sets some context. Sometime, I think it was 1984, thereabouts, maybe 1983, Georgia Tech joined the SURANet, which was the Southern Universities Research Alliance Network, which then became part of the NSFNET. And as part of the grant, the faculty got — or the university got — a VAX 780 computer, which was a pretty big deal at the time. And the deal for the 780, it was partly funded by computer science and partly by the physics department. The computer science department would run Berkeley Unix on it and the physics department would run VMS, so we had to reboot it every night so they could run their programs for particle manipulation calculations.

A group of us had the early Usenet and some of the ARPA mailing lists were on the VAX and I got involved with systems administration and running the software; I mean, this (social media and system administration) has always been an area of interest of mine. When the system would get taken offline and rebooted by the physics department that was a window where the mailing lists, and the mail, and the other things didn't come in so the idea was to try to get the physics folks to agree to switch all their programs to run under Unix. Well, they were in FORTRAN and they were unwilling to; they didn't want to switch because it was critical for their publications that they got these done accurately, and they knew they worked under VMS. So there was discussion. There was persuasion by some of the faculty that they would run a trial. The physics faculty would give us a program, the students/staff would translate the program from the VMS FORTRAN into BSD FORTRAN so it would run and compile. And they could do one of their runs and compare the timing to see how it behaved under Unix. And if it was within I think 10 percent — I don't remember the exact details but if it was within 10 percent of the time — and the same results, then the physics faculty would agree to leave the VAX running Unix the whole time.

I was one of the people who had some involvement with the effort to do the translation, although the details are a bit fuzzy now – I haven't thought of this in a long time. As I recall, as we were doing the translation we discovered that the physicists who had written this were building this big table, and every time they went to do a lookup, they would do a linear search through the table, which is horrendously inefficient. Eventually, the table got to be hundreds of thousands, or millions of entries so this was terribly, terribly slow. So someone rewrote that routine to use a — I don't know — binary search, probably, and we sorted the data or maybe we built it as a tree. I don't quite recall, but it was another algorithm to alter it and make it much more efficient. We didn't tell that to the physicists, however. So when they put their program up to run, instead of taking nine hours to run, it finished in 90 minutes and they were ecstatic because the results were exactly the same. It ran this much faster. So they became Unix converts without knowing exactly why!

I was very involved with maintaining the Usenet news groups, and improving their connectivity --something I eventually did for over a decade-- and getting involved in very early social networking in 1982, 1983, 1984, that time period. So along with that and the physics issue, some of the faculty in some of the other departments would come by occasionally and ask questions about their programs because we'd gotten a reputation, this group, for doing this kind of work. As part of that, I discovered that some of the mathematical results from some programs were not accurate, they were skewed, and we didn't quite understand why.

So I got a book on numerical computation — I still have it, in fact it's on the shelf over there — that had a whole bunch of tests that were nicely written, to test numerical stability and accuracy. I implemented the tests and ran them on all the computers that I could find that Georgia Tech had — and there were about a half dozen different varieties — and found that only one of them had a good mathematical library. Some of them were off 60 out of 64 significant bits kind of thing — only the four most significant bits were accurate, everything else was wrong. So this was something that I was doing at the software engineering center the first few months, and that ended up being my first publication; that was about the stability of those libraries and the report generated quite a bit of interest because people were using these computers for major engineering applications and otherwise.

That experience got me much more interested, along with what I had been doing for the distributed systems and the software engineering, on the whole question of reliance on computers and trust in computers. I had been interested in security all along, but this just reinforced it from another perspective.

Rich also had funding and was working on a form of testing of software called mutation testing, which involves altering a program in predictable ways and seeing what the output is. Give it a test set and the goal is to augment the test set so that all variations of the program can be distinguished from the original. And along the way you build a complete test set. It still is a conceptually wonderful idea of how to thoroughly test software. It is, however, computationally expensive to make all these variants of programs and run them. This is what he was working on, and I was supporting that work and I was heavily involved in that. So those two projects were the majority of what I was doing.

Yost: Can you tell me a bit about your job search, and how you ended up here at Purdue?

Spafford: My wife had finished her program and we had assumed that the research center was going to continue. Rich and those of us who were working with him had actually competed on an Air Force BAA that was awarded to CMU, and resulted in the Software Engineering Institute. Had things been a little different, I would've stayed in Atlanta and the software engineering institute would've been there. Rich had gotten some commitment from the university administration for continuing the center, but it was not the kind of enthusiastic support he was really looking for.

Purdue had just gotten funding for an NSF-funded university/industry cooperative center called the SERC, the Software Engineering Research Center, and approached him about being the head of SERC, the director. Rich interviewed and decided yes indeed, he was going to come here to Purdue. He got a commitment from people here at Purdue that he could bring staff and faculty with him if they were judged to be appropriate by Purdue standards, which were, of course, high; Georgia Tech was still in the ascendency at the time; it was a good school but Purdue was better at the time.

So when Rich announced this at the time, he was kind of, well, "I put all your names in so you can consider Purdue if you want, and if not, I'll write you good letters wherever you want to go." So I consulted with my wife. We picked a couple areas in the country we'd be interested in living and schools that I thought had a good mix of distributed systems and software engineering that I could work in. And I sent application letters off, including Purdue.

First one I heard back from was Purdue, and they invited me to visit and interview. I had an okay interview. I don't know that it was stellar, but it was okay. I'd already known of a half a dozen of the faculty here. It was a very prominent institution; this is the oldest computer science department in North America so it's got a long, storied history to it. And they made me an offer.

It turns out that I probably could have delayed and got the offer extended for a longer period of time, while I waited to hear from other places. But it looked like just a great opportunity to work with people who were here, that I knew, were very good in the field, and Rich was coming here, and we had a good working relationship. So I think we had one round of negotiation on salary and I accepted the position.

About a week after I accepted I got a letter from the University of Maryland, they wanted me to come interview, so their timing could've been better. I didn't hear from other places. Years later I found out that … one of the places I had sent an application to was UT Austin and this was interesting: when I was going for grad school I applied there and, they somehow lost my application. When I applied there for a faculty position, I found out later they lost my application! I don't recall if I heard from anywhere else. So I ended up here at Purdue, ostensibly as a distributed systems and software engineering person.

Yost: This, of course, is the school that Peter and Dorothy Denning were at and did some pioneering work in computer security while they were here. And Samuel Wagstaff was a cryptographer when he was here . . .

Spafford: He's still here.

Yost: . . . and still here. When you came were there others besides Samuel Wagstaff that were in the computer security area?

Spafford: Not in CS, and even if so, it didn't even register for me. All through my undergraduate and graduate career I'd been interested in security. As a graduate student I was consulting on security, but everyone had told me that unless I was doing cryptography or formal software engineering methods — neither of which I was good at and I will still not claim that I am particularly good at advanced creative thought in those areas — that it wasn't an academic career: that I couldn't do it. I mean, this is early 1980s to mid-1980s, and the national community climate at the time was that it'd been shown that testing could never find all flaws. Yet, the "Red Menace" was out there and as a result we had to make sure that systems were absolutely impervious, and the folks who were doing formal mathematical modeling and formal mathematical methods kept claiming that theirs was the one true way that could do this. So all the money and all the attention was going into that. Thus I really was not very much focused on security as a research career path.

The kinds of things I was doing were viewed as support functions or hobbyist functions, even when I came here. I'd already known many of the computing staff here, not just the faculty, and forged alliances and was working with them on things. I was still heavily involved with the Usenet when I got here, and they gave me a role in doing that. The first couple years I was here, SERC got funding, got a number of machines in, and I was put in charge of those, configuring them, doing the security on them just as a sort of an aside. So I was doing it but it was not viewed as an academic pursuit. My first few papers here, my first Ph.D. students, were all in software testing.

Yost: So, now the IEEE Computer Security Symposium started in 1980-81 timeframe. That had to have a significant impact in establishing computer security as a recognized academic field?

Spafford: I would say it did but it was largely devoted to theoretical methods the first decade or so. I remember in 1992, 1993, Gene Kim and I — Gene was an undergrad at the time and he built the Tripwire code. I designed it, he built it, and then I did sort of destructive testing on it, and he went back and rebuilt it. We produced a couple of papers, one of which I sent off to the IEEE Symposium — on Tripwire, on things that we had found while running it and distributing it to other sites. The reviewer comments that came back said "They've built this and it works, why are they submitting it to this conference?" Which struck me very oddly then and still does. From my point of view, they were not interested in things that worked, they were interested in proofs, for an awful lot of the early years; they wanted theoretical results.

I’ve since had work with students published at that conference. I’ve never attended it; I’ve yet to go to a single one of the conferences. That is largely a funding issue. Whenever I had a paper there, I preferred to fund the students to attend – it’s better for their career.   I’ve never had a lot of money for travel to conferences, and I generally prefer to give my senior students the opportunity to go, because I remember what it was like when I was a student and never had a paper or much chance to go to conferences.

Yost: You published an article early in your time at Purdue, “The Internet Worm: Crisis and Aftermath,” that was a year after the Morris Worm. Can you tell me about the context of writing that article?

Spafford: I’d been here at Purdue a year and it was around this time of year, November 2, which is interesting because that’s also my wedding anniversary. So my wife and I had gone out for the evening, and she threatened me if I got online after dinner to spend any time online. So, for purposes of marital harmony I was offline that whole evening; had no access to anything.

As was my schedule at the time, I got up early the next day, made some coffee, I was having some coffee, sat down and dialed in — this was at the time of modems — to my machine, which was a client off a server machine that was part of the software engineering center’s systems. Had no mail, couldn’t get a response out of the machine, had no news groups. When I went to the server I discovered it was incredibly bogged down with all these processes running that were unknown. I then dialed in to a department machine, which was a different architecture, was running fine. Exchanged some e-mail with one of the staff who was there early, and got the response that there was something odd going on, on the Internet. So I quickly got myself dressed and went into the office, started consulting with some of the staff that I'd had contacts with and found out some preliminary details about this program that was running in the background.

We formed a group locally who were in communication with each other. We found machines that were not contaminated and began working to do analysis of various parts; we each took parts that we could do. The work that I'd been doing in software engineering and reverse analysis of my security work were well suited to this. I knew the Unix system forwards and back. I had one on my desktop, so I did some disassembly. I did background research. There were other people here who also had built a number of tools; some very talented people here locally. Purdue had fantastic — still does — a lot of fantastic people working on the services side of the university and we made some real progress against this. Meanwhile, I cleaned up the systems that I had and was looking for ways to keep them clean and re-establish some of the network connections to the outside. The whole network was really severely disrupted at the time.

I began to get e-mail from other sites, from people I knew. As I said, I had been really heavily involved with the Usenet — starting in 1982, 1983 — and by 1988 I was viewed as one of the leaders of the Usenet community. I was a senior person on some of the security lists, the system administration lists, although I was certainly not the only one — don't mean to portray that — but [pause]

Yost: Who were some others?

Spafford: There was a fellow by the name of Erik Fair, out at Berkeley, and Keith Bostic. Actually, most of the people who were working on Berkeley Unix were involved, and Rick Adams at the Center for Seismic Studies at Virginia. He went on to found UUNet, so he was very heavily involved in that arena. A number of people who were with AT&T, like Steve Bellovin, Peter Honeyman. So there were a lot of people like that who were out in various organizations that connected by Usenet, and in that community, who were very well known.

But I started getting e-mail exchanges with people at a couple of universities and we were exchanging information, so I set up a mailing list as I heard from people both local and remote, where we were exchanging information. I named it "*phage*." Then our group locally discovered… well, first the folks at Berkeley published a patch that was supposed to stop the worm and it didn't work in every case. We came up with one that did and published it widely on the list. And then I think I turned it into a Usenet news group because I had the authority to create news groups to collect and share information.

Then I started the process of complete disassembly of the code the next day, making notes as I went along as to what it did and how it behaved. Using the information from the list and my own analysis, I started writing up a document as to how the code behaved, and shared that with some people on the list. Steve Bellovin, who's now at Columbia, suggested that I turn it into a paper that described fully how the thing worked, how it behaved, because other people would be interested in the analysis. So I included other information in the report, put a Purdue Technical Report number on it, and put it out for FTP. There was no web at the time. And wow! It was very widely adopted.

I got an invitation to do a summary version of it for *Communications of the ACM*, which I did, and received a tremendous amount of coverage. I was somewhat surprised by that, actually.

It's interesting that John Markoff and his then-wife, Katie Hafner wrote a book about hacking including the Internet Worm and in the book, labeled me "an opportunist," which hurt a little at the time, but I think was very interesting. I mean, that's kind of ironic to do that considering that they were taking advantage of all the publicity about worms and viruses at the time. [Laughs] They had never interviewed me, but I had been working in security for over a decade prior to that. And publication of results is an integral part of what I'm supposed to do as a faculty member! Yes, well, it was an opportunity but it wasn't like I just suddenly changed things midstream and got launched into that, so I was a little surprised. I was working at the time. I had a couple students, we were doing software engineering research. I was writing on that software research. I was involved with the joint ACM/IEEE Task Force on Curriculum. So I was fully engaged, other than this. There's an anecdote here that I'll relate, then I want to take a break to go get some water.

At the time, John Rice was the department head here, and he had a policy that tech reports were free to anybody who wanted them when we produced them. We'd mail them out at people's request. Paper was still the common format – this was way before the WWW. We had just begun to produce some in PostScript. I don't remember if PDF was widely used then or not, I think it was, but we would make them available online if people wanted them.

So I had it up on the FTP site; a lot of people got copies. But we also sent out a lot of paper copies. It still holds the record of the most copies of any tech report the department ever produced. The final number that I heard is they produced over 1900 of them that were mailed out in the first six months, which is a fair number.

The technical report librarian was a woman named Peggy, and Peggy had been here for ages. She'd been a secretary and support person for a number of faculty as well as the librarian. Walter Tichy had been on the faculty here years before, and he was now a senior faculty member in Europe; he was at University of Karlsruhe in Germany. And he wanted to get some copies of the report for himself and to share with his colleagues. He had been on the faculty here so he knew the procedure and he knew Peggy was the one to contact. So he wrote a letter, not to me but to Peggy, asking for six copies of the report. Well this had been after about three months and already a thousand of these had gone out. And so John had told Peggy to ship all reports out without covers on them because the covers were like 50 cents a report – they were specially printed cardboard — and it was getting to be quite expensive so just do the copying and save on the postage, and so on. When Peggy got the request from Walter, she took six copies of the report without the covers, put them in an envelope and sent them off to him … by cheapest method: surface mail.

Around that time, I was also playing practical jokes — well, I always play practical jokes, but — around April first I played a pretty good one that looked like it was a fake letter from the FBI to several of my colleagues that asked that they call the agent in charge, whose name was Theodore "Teddy" Baer. And I had the phone number of the Indianapolis Zoo listed as his number. Many of them fell for that and called the zoo asking for “Teddy Baer.” It was pretty funny, but some of them were threatening to get me back. So when May came around and I got this phone call from someone with an accent who said, “Where’s the camera-ready copy?” I thought yes, sure, said “I’m not falling for that” and hung up. The person called me back: “No, no, no, your papers we want to know where the camera-ready copy is.” And I said, save it for next April first, it’s not very funny and hung up again.

Rich DeMillo came to my office and said, “You keep hanging up on Carlo Ghezzi! He’s calling long distance; where’s the paper? You owe him a paper.” I’d never corresponded with Carlo Ghezzi! I have no idea what you’re talking about!

What we sorted out later was that Walter was also chair of the European Software Engineering Conference, which was a big conference. Papers submitted to the conference were supposed to be submitted six copies to be circulated to the program committee. So when an envelope arrived, many weeks after he’d asked for it because it went surface mail, and his secretary saw six copies inside, she thought it was a submission to the conference so she sent it out to the program committee and they accepted it as a paper! Which still I wonder at, I mean, that implies that none of them had read the condensed article, which was in CACM. But the tech report was accepted at the conference, and apparently the letter telling me that it had been accepted at the conference had gone back to Peggy and she hadn’t forwarded it to me so I never knew that it had been accepted at a conference I didn’t submit it to!

So over the next few days, I furiously wrote a new paper on roughly the same topic that was published, and has also been printed widely; it was, I think, a pretty good paper. But I had no money to go to this conference because it was outside any of the things that I was funded for at the time and there wasn't any funding for a trip to Europe, so I wasn't going to be able to go present the paper. But what then happened is the IBM Users Group Europe invited me to go present at their conference two-and-a-half, three weeks *after* the European Software Engineering Conference, and they would pay for my transatlantic plane ticket, which was significant at the time. So I sent out e-mail to all the people I knew — a bunch of people on the Usenet mailing list — saying, "I've got this conference, and I've got three weeks in between, or two weeks in between, where I'm willing to give talks if you'll cover meals, transportation, and housing." I filled the two weeks. In my mind, I was thinking I'm going to be speaking in England, I'll travel by train to a couple places, I'll end up in Amsterdam, and everything will be great.

It turns out that I had to go from England to Tromsø*,* Norway; to Milan, Italy; to Amsterdam; over to Germany; then to Paris; then Sweden, then… it was a hellish two weeks of harried travel. I gave something like 15 talks in two weeks but it was a side effect of my analysis; it was one of the side effects.

A second side effect that occurred was because I had been studying malware all along, although there didn't seem to be much opportunity to publish on it. I had been studying security, as I said, as a practical matter. I was interested in protecting machines. I was looking at practical security. I was contacted by ADAPSO, which was a trade organization and has since been taken over, it's now the ITAA.

Yost: We actually have their records at CBI.

Spafford: Some of their leaders asked if I would work with them to produce a document describing malware for their users. So I ended up writing the book, and I got some help. My wife was actually the technical editor on that, she helped with the writing. And I found somebody in the UK who I had worked with, and I believe since has been named an OBE and worked for GCHQ, he's a significant figure over there: David Ferbrache. I haven't been in touch with him for years, but he later wrote this great tutorial-type book on computer viruses, what was known, how to stop them.

Our book included, for the first time, documentation on legal issues, the social issues, and it was the first English language book on computer viruses. And ADAPSO distributed it free to all of their members. So I didn't really make any money off of that, basically, but I did get back a real opportunity and all of that was kind of a fallout from the Internet Worm, where work that I'd been doing all along suddenly became very relevant for a larger audience.

[BREAK]

Spafford: So after the ADAPSO book came out, and had generally good reviews, I had some invitations to go speak about malware. I also had a number that were going on after the Worm incident. In fact, one of my first speaking invitations was at the National Institutes of Health. They wanted to understand what a computer "virus" was, which I thought was pretty amusing.

I realized that the combination of things that I knew about — how to practically secure a system, and my ability to write it in a conversational style — was a good matchup.

Meanwhile, I had been conducting research. I graduated several Ph.D. students who were working in software engineering, mostly testing, and I had a couple of undergraduates who approached me for projects. And one of them, Dan Farmer, I gave him the project for the COPS scanner as a summer project, which he did. We got a couple papers out on that, and became very well known. I insisted, as a first principle, that he write tests that would look for problems without actually exercising them. This worked really well, and is unfortunately not respected by too many people in the field now.

Gene Kim had also come to me for a project, and I've written about this in my blog, about what was involved in getting to the point where we had a releasable version of Tripwire. And that was also very well known. That was in the 1990-93 timeframe, in that era.

But about 1990, I think COPS was out, I don't think Tripwire was out, but I had gotten the virus book out. I thought well, maybe I ought to write a book about practical Unix security. And Unix was by far, the prominent researcher-oriented OS in use— it was not a desktop operating system, it was a common research environment, academic environment. I contacted O'Reilly Publishers, because I had several of their books and was interested to ask about the feasibility of that. It turns out that Simson Garfinkel, who was a tech writer/columnist/software developer had also approached O'Reilly about doing a security book. And so the editor said "well why don't the two of you work together? You have complementary skills and abilities."

So that began our collaboration writing the book. It wasn't until a couple years after the book was published that we actually met in person. It was all done by phone and e-mail. We wrote that book and it came out in 1991. When the book came out, I remember going to the National Computer Security Conference, which was being held in the Baltimore-Washington area regularly, at that point. Simson and I have been friends ever since – almost 25 years.

Yost: Had you gone to that conference before then?

Spafford: I had not gone to it before that, as I recall. There was a book signing, and a couple of colleagues introduced me to people; I signed books. Becky Bace was one of the people who I met there and signed a book to her. We got to talking back and forth about intrusion detection and detecting malicious behavior. She invited me to some workshops that she was holding that were being done with the Department of Energy out in Albuquerque. I don't remember the exact order of events — I'd have to go back and consult records, but I became part of the group that was invited. Karl Levitt was involved in this; Dan Farmer, who was now at the CERT at that time, was involved; Becky was helping to run it; Matt Bishop was involved; so as a fellow by the name of Steve Smaha, he was at Haystack Labs, and others, although it was a small community.

Yost: Were some of the people from IDES and NIDES involved at all?

Spafford: Yes. Karl Levitt was . . .

Yost: Teresa Lunt?

Spafford: Teresa Lunt was not involved at that time.

Yost: Dorothy Denning?

Spafford: I don't think she ever showed up at any of the workshops, but there were some others. I'm blanking on the names at the moment, but I know those two weren't. And after listening to some of the conversation, I ended up writing a proposal — it was a brief white paper — that Becky funded. She was at the NSA in the research group and funded the research, and that led to development of the first prototype of what we called IDIOT [Intrusion Detection In Our Time], as an intrusion detection system. And we proved some formal bounds on intrusion detection, that interestingly, have not been referenced very much subsequently, but it established some ground truth for how to go about doing intrusion detection.

I used that work to make an application to DARPA, where Teresa was at the time as a program manager. I got an award to do more intrusion detection work that I used as leverage to build the first COAST lab. That was the funding for the original COAST lab. But it was rocky because Teresa was evidently being pressured by some of the management there at DARPA, and she was in turn pressuring me. She wanted a modification in the statement of work of the proposal to do something that was scientifically, theoretically impossible. It was an intractable result that she wanted me to state that I would try to solve and I refused to do it, so my funding got yanked at the end of year one and left me with a bunch of students and no funding. I had been working with the SERC — now this was 1992 when this happened — so I had [pause]

Yost: So it was 1991 that COAST was launched? Or was that 1992?

Spafford: No, it was 1992; it must have been 1993, because COAST was launched in 1992. I had been working in SERC and doing software engineering research, but despite the fact that we had produced some really nice results, we couldn't get transitioned to any of our industry partners whereas the work I was doing in security, I was getting lots of interest from people outside. The virus book, the Practical Unix and Internet Security book, the talks I was doing — industry really wanted to know about these. So I thought well, I'll put more focus there.

I talked to some of the industry partners that we had through the SERC to say I'm going to be doing this separate thing in security, are you interested in supporting it? Several were — Sun, Microsoft, Bell Northern Research, Bellcore, a few others — so they gave me money to enhance and build the COAST lab out further. And after I graduated my existing students I had in software engineering, I didn't go back there. It's interesting to me to note, though, that some of the people now working in some related areas are beginning to reference the software engineering work that I did 20 years ago. I'm happy that it's being used, it's taken a long time really for some of that, it seems, to be recognized.

Yost: You spoke of some bounds, can you expand on that?

Spafford: The bounds in intrusion detection?

Yost: Yes.

Spafford: That work isn't the one that is now being referenced; that was not software engineering. But the limits on intrusion detection having to do with the kinds of events that can be detected from evidence, pointing out that without actually having a policy you can't tell the difference between a mistake, an error, or an intrusion of certain kinds; that the events on the computer only show you what happened, not why they happened. And up until that point, there'd been a lot of talk about systems determining if somebody was intruding or not by looking at vast amounts of data. We made it very clear that even with historical trends, somebody can be making the same mistake repeatedly because they misunderstand the system; there's no way to know for sure.

So we tried very hard at that point to limit expectations of what others were selling. And that was one of the reasons I think I had the run-in with DARPA. I think the statement was "attempt to find all intrusions on protected systems." It can't be done. There's no way to gather the data or know what that is. You still hear vendors make the claim that they can.

Yost: With the start of COAST, was Wagstaff a colleague that got in at the beginning?

Spafford: Yes. When I first started doing the writing and doing some of the other things, Sam had been teaching a cryptography course here all along, and I turned to him as one of my two mentors here in the department and asked him for suggestions and advice.

Sam's work has always been somewhat solitary. He's a very brilliant number theorist and cryptographer; just absolutely wonderful stuff. Sam, however, just as a mathematician is largely focused on the mathematics and doing the proofs and things separately, he's not systems oriented. So he never was really prominent in the overall community but he's always been a collaborator in things that have gone on and a supporter of this kind of work.

Yost: And did other faculty members join the group early on, or did that take a number of years?

Spafford: Over the next couple of years, there were two, three other faculty who got involved. Mike Atallah, here in CS, early on, after I had produced my first Ph.D. student, and in discussion with one of the funding agencies, we got this idea about searching log files for a particular kind of pattern of events. But I couldn't find anything in the literature about a search algorithm that would handle it. It was one of arbitrary deletions over time in the middle. So I approached Mike as an expert in algorithms — Mike has been a friend and mentor since I've been here — to ask if he knew of any algorithms that were involved in this. He did not, and he found it intriguing that here was an area where he was expert in algorithms and I was posing a problem that had not been addressed. So he started getting involved and the more he got involved, the more problems we were able to identify that he was able to get involved with. Over the long term, he has produced Ph.D.s in the area, a number of papers, and he spun off a startup company that recently got sold, so he’s had great success in the area. But it all started with this question of, do you know of an algorithm that does this?

Another collaborator was a faculty member over in our electrical and engineering department, Carla Brodley. And she worked in knowledge engineering and AI techniques, and was very interested in user behavior as a way of predicting misuse of one kind or another. So I got her involved in that. She is now at Tufts University.
There were some folks in political science that I talked to, but as that was happening, the COAST lab, which was really just within CS, started including faculty outside of CS. And the courses that I wanted to develop and the research that I wanted to do that people were interested in, was — we were beginning to get outside of strictly computer science. That posed a bit of a problem because this is a very traditional computer science department; always has been and still is. Many of the faculty don’t always look at things outside the realm of pure computer science with a favorable attitude. So if I was going to get involved in things outside of computer science, it couldn’t be a lab anymore inside CS. There was considerable pressure on me to alter or moderate the kinds of things I was looking at.

Yost: And so did it become independent of CS? And if so, when did that take place?

Spafford: In 1997, over the summer, I was invited to visit at Georgia Tech, I think to go — well, no, that isn’t how it started. Nineteen ninety-seven, I ran into and met in person, for the first time — someone I had known electronically — Peter Freeman, who was the dean at Georgia Tech. And I had also gotten a letter of encouragement or introduction from the person who had been my master's thesis advisor and was on my Ph.D. committee, Phil Enslow, who was on the faculty at Georgia Tech, and he encouraged me to meet and talk with Peter. Peter had recently, only a couple of years, been made the dean. The department at Georgia Tech had been reorganized as a college and he was the first dean.

One of the things that he wanted to do was have an event that would put computing and its application on the map. And the college — the university, Georgia Tech as a whole — had an offer from Sam Nunn, who had been a Democratic senator from Georgia, very senior, very well-known, that he would lend his presence and support to an appropriate event of some kind. Peter had decided that computer security would be a good event, because Senator Nunn had been in charge of hearings about some events that had occurred, some cyber penetrations; in fact, Nunn's staff were the ones who coined cybersecurity as a term. I remember having a discussion with the senator about whether it was a bad term but one seldom wins arguments with senior senators.

So they were going to have an event, IBM was going to be behind it. The problem was that there was nobody at Georgia Tech who knew anything really about information security so Peter wanted to know if, as an alumnus, I would be willing to help them in putting the event together. And I said sure. I've always been willing to try to help others develop in this area.

They flew me down to Atlanta for a couple meetings of a program committee, various ones, and I basically designed the whole agenda for them. At some point — January or February, one of the near-final meetings. I remember sitting in the room with about seven of the Georgia Tech people and I guess I was rather naïve at the time in all of this, but one of them said you know, this is going to be a big event. We're going to have a lot going on. We need to maintain the momentum somehow. And somebody said yes, what we really ought to do is we ought to establish some kind of a center or something in this area and announce it, and announce a new director. And another said yes, that's a great idea, I wonder who we could pick. And they all got quiet and looked at me, at which point I realized this had probably been something they'd been planning for a little bit longer.

So I talked with them about it, and mentioned a bit about the salary and benefits here, cost of living, how much research money I had in play, and so on. My concern was that if I was going to move, I didn't want to take any big cuts in what I had available for research, and Atlanta is a more expensive place to live than West Lafayette!

The decision, apparently by the provost, was that what was required to move me was too much for someone who was "unproven" – that was the word I heard later from someone. So nothing happened with that situation except word, apparently, got back here and the provost here, Bob Ringel, called me in and said, "Why would you want to leave here?" I said well, Atlanta's a big city, there's a lot going on there, and I've got this lab and my colleagues are not at all happy that I'm looking at broader issues. He said well, there's a solution to at least that, we can create a university center.

So he and the president at the time, Steven Beering, authorized creation of a center, they allocated startup money and space, and in May of 1998 we announced the formation of CERIAS as a university center. I'm pretty sure that they did not anticipated it would grow as large as it has. Because had they thought about it then, they would have set it up as a university institute reporting directly to the provost. Instead, it's a center that reports to a dean, even though the majority of the faculty involved have no reporting line to that dean. So we're oddly positioned within the university, it's never been quite right.

As an aside, Georgia Tech hired someone to head their center who didn't last as the director for very long, and who had no prior experience in academia – he wasn't even hired as a faculty member, as I recall. It was a messy parting.

Also, they also left my name off all of the materials for their Nunn symposium and never credited me at all with helping with the event or starting their center. I thought that was rather petty.

Yost: And what about undergraduate and graduate courses that pertain to the center, was there an education component at the start or were students aligned with different departments?

Spafford: Well, Sam and I, and a few other faculty, did get some computing security classes that were CS classes on the books. Other faculty in ECE had courses on the books; there was, as I recall, even a network security class in our college of psychology. So there were classes out there, and there were students, but all at graduate level. So that was seriously, really, a graduate entity and has been for almost its entire life span.

But the formation of the institute was something where we had seven initial faculty who were part of that, that we had identified. We had about six corporate entities that were partners at first. I spent a fair amount of time studying centers here and at other universities to see what it took to be successful. The startup money that I got from the provost, I used to make two staff hires as the first aspect of what I did. The first was a development person. And the second was a managing director who had a business background and a science background — business and science — who happened to be a next door neighbor of mine and was working in the CS department, so I had known him for some time. Both of them were in the CS department.

So CERIAS got off the ground in May of 1998 and an alumnus that I had met, who I'd told about the center and what we were trying to do and he'd known what we were trying to do through COAST, was friends with one of the directors of the Lilly Endowment in the state. He approached them and said oh, this is really exciting, this is new, you really ought to look at this. So they invited the university to submit a proposal for funding, which the provost said yes, we've got to do this.

I was involved in writing a proposal that was cut back from my original thoughts of what I wanted, then they layered on some extra money for other initiatives that they were doing at the university, so there was a "tax" involved, of sorts. But the Lilly Endowment funded it in December of 1998, and basically, that provided $4.5 million to CERIAS over the first three, four years.

So for the first three or four years, using that money, my director of development, Andra Short, and I spent a lot of time going around to various companies to get them involved, to find internships for students, research problems for the faculty, some other funding for projects. I also hired some staff, including a K-12 educational development person; another person for community outreach and adult education, and she was in the process of finishing her Ph.D. I think both of them were finishing their Ph.Ds. And then shortly thereafter I brought in as a research scientist, Marc Rogers, who had recently finished his

Ph.D. in Canada. He'd designed his own degree program. He had been a detective for several years, got interested in cyber crime, and wanted to do that. He got interested in coming here because I basically had written the first papers on cyber forensics so he wanted to come work on that. There were others, but those were some of the more senior people.

Originally, we had a staff of about 15 part time and full time people. I was out getting industry support and in our very first strategic plan that we did, we identified that there weren't enough people in the U.S. in total to staff a large program.

In 1998, I did my first congressional testimony before a House committee, and it was on precisely this fact — that as of 1998, the best figures I could come up with by polling everybody I knew in the country at that time, that worked on this, was that in the U.S., we were producing three Ph.D.s a year in the field and two of those Ph.D.s were thereupon leaving the United States, going back to a home country, or going to work elsewhere in the world. So it was a terribly, terribly small production. As an aside on that, I proposed some things in my testimony that could help the situation; one became the NSF Cyber Trust program, and the other was the genesis of the Centers of Academic Excellence program.

As we were doing the planning, we realized that we would have to get faculty in other allied fields interested in security. And so the way we did that was through a seed grant process, where I would take some of the Lilly money and offer it up in small increments for them to do exploratory studies, to get something started and then they could go to NSF or elsewhere. Couldn't fund faculty salaries with it; [it] had to be funding students and equipment. Lot of faculty took that up, became interested in the field and went on and did more. Others took the money and ran. That's the nature of any program like that. Of the people I hired, what's interesting is the K-12 person finished her degree and went to Indiana University as a faculty member teaching IT to teachers of K-12. Melissa Dark, who I hired for the continuing education program got her Ph.D., joined the faculty and became an assistant dean over in Technology. She's now a chaired professor there, does work in cybersecurity and evaluation, and works with us still. And the person I hired with his new Ph.D. in cyber forensics, he is now a full professor in technology and is internationally known expert in cyber forensics. So we gave him a platform to go off. He's written books; headed things; he's been chair of the American Association of Forensic Sciences Digital Forensics Section; and all kinds of good stuff. So I had some really good hires, some really good people that I was able to bring in with that money. But within four years it was gone and so we fell back to what the companies provided us.

Yost: So industry has provided continuing support.

Spafford: Yes, at a modest level.

Yost: For federal funding agencies, were they part of the funding model also; with COAST, before the late 1990s, and then the late 1990s and beyond with CERIAS?

Spafford: We tried. We've never had a lot of luck with federal agencies. NSF only does things through competition, competitive funding, and for a long time they had no programs that really funded security research. Throughout the 1990's, there was really nothing there that would do that. And what I needed most was support for infrastructure, personnel, and they don't fund that; they don't do that. So from — and the same is true of ONR, AFOSR, the other federal agencies like that — so we never really got any large scale funding that would let us take large next steps. We got some funding for research projects from the NSA, and the Air Force, a few like places that, but it wasn't large and it was inconsistent.

After transitioning to CERIAS, we had national labs, occasionally, that have been members of our partner consortium but their budgets are such that it's not easy to do that. It's just not a model that seems to work well for them. So we have, off and on, various federal agencies that have been involved but it's very difficult for them to get involved, both because of structure and politics.

Generally, if you're not around Maryland or upper Virginia, if you're not within an hour's driving distance, they're not interested in putting the money in and we're in flyover territory here, despite having the biggest program in the field, and one of the longest running. So it's never been something where we've gotten any significant funding for the center. Our faculty had been very successful in competing in calls for proposals and regular funding programs, but not overall in the kind of big grants that require some stronger connection based on location or politics.

Yost: You mentioned the Air Force and I just wanted to get your perspective. They, of course, did fund a research program in computer security — a bunch of money went to

MITRE. What was your perspective of that work that evolved into TCSEC in certifications and setting the criteria and evaluation infrastructure?

Spafford: At the time, I really was quite dismissive of it. I was not a fan of it because it moved slowly, it created a big division in the marketplace so there were systems that were secure and those that weren't. And for those reasons, I guess I didn't really hold it in high regard.

As time has gone on and I've gained more of an appreciation for what was accomplished, I still think they missed the boat [but] for different reasons. I think the fact that they focused on confidentiality really more than anything else is one of the reasons why it didn't have the commercial application, it didn't reach a wider audience. And the government has had a tendency that they do all or nothing certifications and builds. This hurt them in several places; ADA, for instance. When ADA the standard was developed, they would not allow subsets of ADA, it had to be the full implementation. So it was several years after the standard was issued before there was a fully compliant compiler, and it was so large and expensive that it was very difficult to use in academia. So ADA largely failed, as an effort. That was also an Air Force effort.

The TCSEC, I wouldn't say it failed*, per se*, it did produce some good results. It did produce some good systems. It produced a lot of people who knew how to build better systems that still, you find in isolated places. But it really failed to change the marketplace because it was so cumbersome, and it was so narrowly focused, it didn't have the broader scope. But there was some really excellent work done with it.

Yost: You mentioned that your first National Computer Security Conference was just a book signing with the ADAPSO-distributed book. Was that a conference that you regularly attended after that?

Spafford: I went to it fairly regularly after that.

Yost: Can you give me your impressions of that as a conference then, and how it evolved?

Spafford: It was a combination of conference, trade show, and circus, that basically everybody went to because it was great for networking and finding out what vendors were doing. I spoke, I presented papers, I had a number of papers published in the proceedings. They were good proceedings; there was really some good work that was presented there; and as an intellectual environment, it was wonderful. I remember a half dozen instances of things that came out of meetings there.

At one meeting I had with Tim Grance, who's at NIST and has been there for a long time; I knew him as a grad student. — he signed up for that course that I offered when I was there. He was a young USAF captain who was getting his master's degree at Georgia Tech and he signed up for the course so I knew him from way back. He's been a valued friend and colleague ever since. He's been on the CERIAS steering board from the beginning. I remember talking to him about some of the problems they were having, and suggested to him the idea of a national software reference library, the NSRL, which was basically collecting the cryptographic signatures of files that were allowed on systems.

Then at that same meeting, Mark Pollitt, who was then at the FBI, was talking to me and Tim, and saying this is a way you can use to search computers, this is what's involved. That was about the time that I published the first real forensics paper, and so Mark took some of these ideas too, and he was the one who founded the CART, the computer analysis lab at the FBI. I'm not claiming responsibility for that but some of those ideas that we discussed found their way into what he was doing.

I remember meeting Stephanie Forrest at the conference and talking about biologically inspired defenses, which she had had as an idea some time earlier; she used the conversations as inspiration and did wonderful work in the area. She had the idea before talking to me. I mean, she sought me out there, but she's done great work in that field and that's where I first met her.

I met Willis Ware there for the first time. I met Harold Highland, the late Harold Highland, who was the founding editor of the *Computers & Security* journal, and he was very encouraging to me as a young researcher and invited me to submit to the journal, which I did on a couple of occasions. I have succeeded him now as Editor-in-Chief of that journal. There were many more, but that's just a few off the top.

So I had a lot of great meetings. There were a number of people there that I met from law enforcement, from government, from companies. RSA does a little of that but it's not quite the same atmosphere. The trade show was always interesting because of a lot of the software, it is a little bit more like RSA now, except generally you had engineers there because they had to answer questions, it was not just marketing. I got an opportunity to try or look at a lot of hardware that we didn't have here.

But there was also a circus atmosphere and there was also a narrowness of view. I remember there was one panel that Steve Bellovin and I were on; I know we weren't the only panelists but I don't remember who else was on it. The name of the proceedings was "Challenges of the National Information Infrastructure," which was a buzzword in the mid-1990s, the NII. I was the penultimate speaker on the panel, as I recall, with Steve last, and I started off — it was a fairly packed room — by saying the biggest problem is you don't understand what it is. It's not the *national* information infrastructure but *global* information infrastructure. The Internet is not a U.S. phenomenon or artifact. Everybody else had been talking about it that way for the whole conference and I actually got some pushback from people about my comment — "But we invented it, it's ours, that's what we're supposed to be doing." [Sigh.] Okay.

So there was that element of the conference; there were people who really didn't understand well, but Jack Holleran, I don't know if you've run into Jack's name.

Yost: No I haven't.

Spafford: Jack was the person at the National Computer Security Center that co-organized this conference every year. I had a deal with Jack. He would give free admission to any of my students who agreed to work as ushers or information desk people at the conference. And so by the time we got to 2000, I think I was bringing a dozen students at a time to the conference. And they loved it because they got a chance to meet with industry people. They got to see the equipment. They got to meet with luminaries in the field. It was a wonderful adjunct to courses and research here. I wish there was a conference now that I could do that same kind of thing. Jack's contribution to some of our growth was just incredible.

As I recall, 2000 was a year unexpectedly, for me, where I got the National Computer Systems Security Award, and it was presented to me by Mike Hayden, who was the director of the NSA at the time. I'd been consulting at the agency; I'd never met him, though.

He and I had discussion over dinner of what he had hoped for the agency and what I was doing, and what I wanted to do. And he made an offer to me that if I wanted to come to the agency on an IPA, he wanted to create the role of Chief Technology Officer, which had not existed there before. And he thought I'd be a good person for that role, where what he wanted me to do was to go around to the agency, and look at all the things they did with computers, and make some recommendations on how to modernize and economize what they were doing. I had a sabbatical coming up so we did some back and forth about how to do that with an IPA, for me to go there for a year. I finally got permission from the university, and I was getting ready to sign the paperwork.

Around that time there was a meeting at the NSA – they were playing host to people from all the national centers of excellence, the university centers, including ours. But anyway, they were hosting it. I was going to go there and I had this letter that I just had to sign to finalize the IPA that would start in December and would run for a whole calendar year. So I decided I would talk to the folks at the agency when I got there to make sure everything's still good, and I'll sign it when I get back. Plus, I had to rush because my father was living in that area — my sister was living in that area [and] my father was living near her — and he had just had a stroke. So I needed to get to the Washington area as quickly as possible. So I got to Washington, visited my dad a little bit, went to the Centers of Excellence meeting at Fort Meade, and while sitting in the conference room — and this is a very clear memory — we're waiting for a gentleman by the name of Larry Castro, who was the person in charge of counterterrorism for the NSA, to come and give us a briefing, faculty from all these universities. I was sitting next to Peter Freeman, from Georgia Tech, who was there and we were told Larry was delayed.

Somebody said, turn on the TV. We turned on the TV and there were these news accounts of planes that had crashed into the World Trade Center. I was sitting in the situation room at the NSA waiting for a briefing on counterterrorism as 9-11 unfolded. As we were leaving the building — they ordered an evacuation because they didn't know if the NSA was going to be a target — as we were headed out to the car, the TV in the lobby showed the plane crashing into the Pentagon. We knew the world had changed drastically.

I was in Washington for a week and then got a rental car and drove — after I found where my father had been moved as a result of the 9/11 aftermath, and situated — I drove back here to Indiana. I wrote a note to Mike Hayden saying, based on what's happened and what's likely to happen, this seems to drastically change the environment. I don't think it would be the same environment that you had in mind. He sent back the letter with a note in the margin that said, basically, I don't think you should come.

So that blew that sabbatical out of the water, and that was the last national conference. They didn't do one after that. In retrospect, considering some of the things that occurred and some of the things that went on, it was probably the best recommendation not to have gone – some of the massive data collection started as a result if 9/11. I wonder what would have happened had I been exposed to that; I would not have been happy with many of the things that went on immediately after 9/11. That was also when they cut ties to a lot of academics. So that was my experience with the national conference and a follow-on as to [pause]

Yost: Right. You brought up the RSA Conference. That started as a conference but evolved to a huge trade show. Was that something that you attended with any regularity and was that useful?

Spafford: Not, not with regularity. I've never had a lot of money here to do things that I'd like to do. The funding that I've had I've generally plowed back into the center and I haven't kept a large fund of my own. So going to conferences that charge a lot of money, and flying out to San Francisco, and so on has been a hardship over the years. Things are a little better now. I have a small amount of money that I can do this, and RSA has been one of our partners in the centers so I sometimes get reduced admissions. But I would go to RSA sporadically, every couple of years. I've gone for, I think, the last four years straight — sorry, the last three years straight — but in the early days I only went occasionally. And in the early days, they offered no academic discount, and so it was full price. It was really more trade show than it was conference and it was just too expensive to go to.

Yost: You brought up Tripwire and I'd like to ask you a little bit more about that. That was a Unix file integrity monitor, and it was distributed as a no-cost tool and was used on thousands of systems world-wide, as I understand it. Was that the first really widely distributed intrusion detection tool out there?

Spafford: To my knowledge, yes. I've never seen evidence of anything else that's been as widely used. The genesis of that — I had for a while been building sensors and detection on my systems. I became a bit of a target for people after the incident of the Internet Worm. So I actually built a totally fake decoy system on a Sun workstation. It looked like my computer. It had a lot of files and mail and things on it. It was totally bogus. It was just a honeypot, although I didn't use that term at the time.

I had some of the internet worm code there that had been neutered. So for instance, I had the encryption routines there. I had something that would compile but it wasn't complete. The encryption routines were there but I had altered the tables so that they wouldn't work properly, and a number of other things. But it was a convincing fake. I'd gotten that idea from Cliff Stoll. With the Cuckoo's Egg that had occurred a few years earlier, I knew Cliff from my days at Georgia Tech. You'll see I'm mentioned in the acknowledgements in his *Cuckoo's Egg* book.

So I had this system up and running, and I would monitor it regularly. There's a book called *Hackers* by Suelette Dreyfus that came out that details an account of a couple of guys who bragged about getting into my system and getting a copy of the Morris Worm. Well, she never did any fact checking, she never did any background on that for the book, and I've written about this on my blog a few years ago. What happened is they broke into my decoy system, they got the doctored version of the code. What was particularly ironic about it was that while they were bragging about breaking in — while they were doing the breaking in from Australia — I was in Australia and I was visiting the national police who were showing me the transcripts of them breaking into my system. So I was able to identify to them right up close what was going on, and logging in to get the logs from my system, which were subsequently used to arrest these guys so it was really quite amusing. So the story is out there that people broke into my system and stole a copy of the worm, but that is not what happened.

I had that system instrumented and I detected at one point an odd change in files and the system crashed repeatedly. And that was unusual because there was no reason it should; it wasn't doing anything. When I went back and looked at the logs, I noticed that somebody had installed something in the library on the system — this was a Sun workstation with shared libraries. A cursory look at the library indicated that the date and the checksum were all as they should be, but if I did a binary comparison against what it should have been, it had significant change, including a password that had been built in as a back door. So once this library was in place, anybody could get in remotely if they knew this password.

Clearly, somebody had exploited a flaw to get into the system and was installing back doors, cleverly engineered to evade the checks that a COPS-like program would run. It turns out later the intruders were the Infomaster crew. There's a book called *At Large* that documented this, by a couple authors, Charles Mann is the one author I remember, I don't remember the other [David Freedman]. They were doing this to hundreds of systems around the world. Somebody from Israel was apparently also involved.

It was clear that somebody was breaking in and it wasn't being found with regular tools. I had been reading some papers on message digests at the time, and I thought this was an indicator they couldn’t subvert easily if it worked correctly. So I sort of noodled around a little with that and hadn’t gotten very far when Gene Kim showed up at my door.

Gene was an undergraduate and he had met someone I knew, Rob Kolstad, who was very involved in the Usenet community, and Rob suggested to Gene that he come visit me if he wanted a project. I thought, well, this is interesting; let’s see what he can do. So I gave him the task of implementing MD4 I think it was — one of the algorithms — and said try a bunch of files and see if you ever get a collision. Mathematically, it shouldn’t have happened but I thought well, try a bunch of files. So he tried a bunch of files, a few hundred and I said, no, no, you’ve got to try tens of thousands. He said, where am I going to get thousands of files? Usenet, out of the net, whatever.

Gene went off, and he was working at the time as a systems administrator for the campus computing center, and decided that there were lots of files on campus so he could do that. So he ran the message digest function on every file on all of the general user machines that were in the computing center, half a million files, something like that. At the time, it seemed large; I mean, it was a lot of files for campus at the time. And he came to me to report that he ran all these files and there were no collisions. I thought that’s pretty good. About three days later he came to me and he says, I’ve been fired. The reasoning was because when he had run this against all the computers in the computing center, it reset the access bit for every file on every system, so they all got scheduled for the next incremental backup and they blew out the backup tapes. It was then discovered that he hadn’t had permission to run this against all of the files, so he lost his job.

I felt a little guilty about that — not a lot because I hadn’t made that choice, but a little guilty for putting him up to it. So I hired him with some funds that I had through the lab, [and I] had him run more tests and start writing the Tripwire program I designed. When we got it working, I thought this is really valuable, it seems to work very well; let's put it out for people to use and give us feedback.

Yost: Were there other intrusion detection systems that served in any way as a model for doing Tripwire?

Spafford: No, it was just totally home grown. There were some commercial systems that did AI-based kind of detection, and there were some other research programs. There were the things going on at Haystack. There was a system called Dragon at Sandia National Labs, or maybe that was at Los Alamos, but there was nothing like what we had put together.

I've always been focused on trying to help people rather than make a lot of money, so we had no thought of commercializing Tripwire. It wasn't until years later, after Gene had completed his graduate degree and gone to a startup that the idea occurred to him to do a supported, commercial version of Tripwire. It wasn't a university project.

Yost: Can you tell me how you got into the area of forensics? You obviously did some really pioneering work in that.

Spafford: Well, arguably the analysis I did with the Morris Worm, taking it apart, was some original forensics. I had been doing some of that with computer viruses, too. And I spent the next three or four years after that trying to get funding to develop reverse engineering tools, which I thought would be good for the software engineering work I was doing and for security. But nobody would fund it. In retrospect, and what I was told privately by someone, this was discouraged by the National Security Agency. They didn't want people taking software apart, for whatever reasons, and I could speculate but I don't know for certain. Again, this is unproven; this is simply what I heard from people.

But I had discussions with Tim Grance and Mark Pollitt about doing criminal investigation software, and a lot of people turned to me because I had been doing reverse analysis work, I had been doing debugging and analysis work for my software engineering. It got me thinking about the problem more, and I had published bits and pieces of it here and there on the net, more than anything else because I couldn't get the funding to do a full scale project; some smaller hints at this analysis of the library, trying to find out what had happened to my honeypot was another prompt. So there are several things that had happened as we went along.

I had a graduate student that approached me; he was interested in a project. His name was Steve Weeber and he had taken my security class, bright guy, wanted a project and so I thought well, what can we learn about an author by doing some reverse analysis? What are some of the aspects of analyzing code that can capitalize on? So we ended up writing a paper that was presented at the national conference, and then later, an expanded version was published in *Computers & Security*. Harold Highland in fact encouraged me to do that. I believe he saw the presentation at the National Security Conference, and then encouraged me to publish it in the journal on how software can be analyzed to trace it back to the authors of the software. Steve decided not to pursue a Ph.D. and left after getting his master's. I think I coined the term "software forensics" for that paper.

But I had another student, Ivan Krsul, who was looking for a master's project, and for his master's thesis I had him continue the work. And he did some experimentation and so we got a paper out of that, and publications. That then led to Ivan's Ph.D. thesis on "Vulnerability Classification and Identification" that was very widely cited, and served in part as an impetus for MITRE's CVE effort that has turned into a major community resource.

MITRE had independently started that, separate from what we had done but as part of supporting Ivan's work, I had a workshop here at Purdue for people interested in vulnerability classification and sharing, which nobody was doing prior to that time. If you wanted to study vulnerabilities in a system, or attack code, you couldn't get it. Even if they had it, they were afraid to share it. So we wanted to find some way to do this. I got a little bit of funding from Tim at NIST, and we hosted a workshop. As a result of the workshop, the folks at MITRE decided to alter some of what they were doing, and it turned into a public project and that became the CVE Project. And then Ivan went on to finish his Ph.D.

Later, I had another student, Brian Carrier, who had been with us as a grad student then went to work in industry for a while, then came back. He did his Ph.D. with me on a formal model for forensic analysis. It was the first such model, and Brian did a fantastic job – very self-directed. He has written books and a very popular toolset for forensic analysis – he's still a major figure in the field. So did Dan Farmer, my former student who did COPS. So, all of that kind of came out of our shop here.

So all of that was part of my forensic phase, where I was developing source code, and source code analysis methods, and looking at vulnerabilities to try to find ways to reverse engineer them back into code. I developed some tools. I put out the work that I did with Steve and Ivan and Brian. And then hit another brick wall with funding. I tried to get funding from NSF. I tried to get funding from NIJ, National Institutes of Justice, which is the funding arm of Justice. I tried to get companies interested in supporting this because I knew [pause]

Yost: Does the FBI have any research programs that fund [pause]

Spafford: Only through NIJ. They had a little bit at Quantico but it wasn't in this area. It was very frustrating because I wanted to build tools, I wanted to do things, but the reality of the environment here is that doing something like that on my own time doesn't generate rewards. And I was trying then to become a full professor and so that really required bringing in funding and writing papers. That was an area that after about a year's worth of trying, I couldn't get anything.

This is a repeated theme of my career in academia: I have these ideas to do things and then am totally unable to get the support to carry it forward so I abandon it and go on to something else, and then 10 or 15 years later I'd see other people get excited about these ideas and get lots of funding and acclaim. It's frustrating at a certain level, but well, there we go.

However, as I noted, it inspired Marc Rogers to join us, and some other young faculty, and the CVE, and Brian and Ivan's Ph.D. work, and I can take pride that Purdue has produced scores of grads who work in forensics now. That is some measure of success even if didn't go quite as I wanted.

Yost: In the mid-1990s you published some on creating research on applied genetic programming, autonomous agents to intrusion detection. Can you talk about how that got started and how did that idea come to you?

Spafford: I don't know the exact dates, early 1990s, a gentleman by the name of Chris Langton was running some conferences out at Santa Fe Institute on artificial life and when he looked up computer virus he found my name. And he invited me to go present at the Artificial Life Conference, where people were doing a lot with genetic algorithms and programming, and the like.

So I prepared a paper about whether computer viruses are artificial life and presented it at the conference and met some of the people. That paper, actually, was at one time, fairly widely cited. But it got me thinking about the whole issue of are there techniques in this field to apply? So I started reading on genetic algorithms.

Actually I was still interested in finding vulnerabilities and finding intrusions. So I read some on genetic algorithms and I followed the stuff on artificial life, to the point where I was actually on the editorial board of the journal and the conference board for a while. And that lead to what I did.

I had a grad student I was working with, Mark Crosbie, who was interested in this area. We wrote the first paper on using agents for intrusion detection. Mark left with his master's. He's currently in charge of Facebook security for non-U.S. sites, so he's done well. Great guy, from Ireland; we've had a number of wonderful people from around the world work with us here. Security isn't a US-only issue by any means. So Mark and I produced the first paper; it's been widely cited; lot of people found it an interesting approach. Then I took those ideas with Diego Zamboni as the next step to the programming of the system — that's what Diego did. Diego did some great work.

It's another one of the instances where one of my students has gotten some incredible results but was ignored by most people because we didn't try to start a company around it. We found ways to detect attacks that had never been seen before. We could stop zero day attacks with his system.

The down side is that it requires instrumentation in the operating system, so it's not something that people can do on their own. It's got to be picked up by vendors and if vendors don't want to do it, it's not going to happen. So we got all the way through Diego's implementation, the bounding values, everything like that, and there was no way to take it further unless a company like Microsoft, or Apple, Red Hat, or someone who wanted to productize it. So it was not something we were able to do; it stopped there.

Yost: Is that something that you make a pitch and actively try and get vendors to take on?

Spafford: Yes. We have relationships with several to try to do that. It wouldn't make sense to do a startup because, for instance, if we wanted to do Windows, which at the time was the major market, we would have to have Windows source code, we would have to make changes to the Windows system and support the changes. It would not have made any sense to do externally. So I made a good pitch to them and they just weren't interested in incorporating something like that.

Yost: In 2003, you published a co-written article on PFIRES in *Communications of the ACM*. Can you tell me about the origin of that policy framework that you published then?

Spafford: So that was in the early days of CERIAS getting started, and one of our partners at the time was Andersen Consulting. They expressed an interested in how to convey to customers the process of policy development and refinement for security. And they really didn't have anything in mind, they just knew it was something that was needed.

Jackie Rees was a relatively new faculty member over in our management college who had a computer science background but was more interested in the policy side of it. She took this on as a project and realized that she needed more experience with the policy end, so I joined in on it with her and I brought with that my experience working with policy for systems. We iteratively developed the model. A little of it was also inspired by what I knew of the OODA Loop model that was used in — it's taught to pilots in the military, among others.

I had worked on developing policy and refining policy for a number of corporations in the 1990s. [I] was hired by both Shell and Exxon to help refine their security policies, and by SWIFT, the electronic funds transfer people. So I had seen corporate policies up close. I'd been part of the process so I provided a lot of that as input that Jackie manipulated into a more coherent framework that could be described in the management literature, which I was not familiar with — I had the practical experience, but not the knowledge about how to phrase it — and that was a great collaboration. The folks at Andersen, and their follow-on, which I'm blanking on right at the moment [pause]

Yost: Accenture?

Spafford: Accenture, thank you —used it as their engagement model for over a decade. So it was a big success.

Yost: Can you compare and contrast CERIAS with some of the other academic centers in information assurance? A number of them, now, is this still the largest?

Spafford: To my knowledge it is. So when CERIAS was founded there were three other places that had a formal academic entity. They were UC-Davis, University of Wisconsin Milwaukee, and George Mason University. The one at Milwaukee, the dean decided that security was a passing fad and basically pulled the support. The two faculty that I remember who were most instrumental there, Yvo Desmedt, he's now at UT Dallas, and Rene Peralta is now at NIST. So that went away.

The one at George Mason fractured and has gone away or dormant, effectively, with Ravi Sandhu going to UT San Antonio; that disappeared. The one at Davis has held on. That was originally Karl Levitt and Matt Bishop and that is still going strong out there. That's only a couple of people now, so in some sense, CERIAS is the oldest in the U.S. of any size. We trace our lineage back to 1992. Those three places were around when the COAST laboratory was formally formed, but Davis is the only one still holding on.

During the middle years of COAST, and actually right at the initial part of CERIAS where I gave the Congressional testimony and otherwise, it was clear that we had to do a better job in academia. So one of the things I outlined in that testimony was the Centers of Excellence program and the Cyber Trust program that NSF picked up. So both of those were actually in my testimony, in a form. The folks from OSTP met with me after the testimony as did Congressional staff. And both of those programs emerged from my testimony because the basic designs of both are very clear and the people who started them were people who talked to me about it.

So, for other centers… let me think out loud. Davis already had one, George Mason had one, we had one, and there were a couple of others that were nascent that had just sort of started up. Idaho was one, with Deb Frincke and Jim Alves-Foss at Idaho. Deb is now an assistant director at the NSA. I tried to recruit her when she was a grad student of Karl Levitt's, to get her to come here. Didn't happen. CMU is another place that tried to recruit me at one point and decided that I wasn't worth it, and they started the CyLab thereafter. The Georgia Tech center started in about 1998, as I noted earlier, but about 3 months after CERIAS. M.I.T., I think, was one of the other seven. I don't remember if I covered them all but that's basically it.

Most of us collaborated; we all worked together to try to find ways to enhance what we were doing at Centers of Academic Excellence. The original person who presented us with certificates for that was Richard Clarke who was at the Executive Office of the President.

After we got the Lilly money here, I set up a program of academic affiliates because as I said, our strategic plan, we didn't have enough people in the field, and we wanted a mechanism to feed in students as well as place our PhD grads in faculty positions, so I made arrangements with a bunch of universities — Iowa State, Georgia Tech, Maryland, North Carolina State, Utah, I think Utah, one in Texas, a couple of other places. And also University of Milan, in Europe, and QUT in Australia, that, as an affiliate, we would host their tech reports and Ph.D. theses on our web server if they would provide a link for CERIAS to our site. We'd give them discounts to come to any events we had. We consulted with have them as part of our curriculum efforts — we haven't talked about that yet — to try and get some common curriculum in K-12. And that we would host them, host their students and faculty in our seminar series. Some other things like that.

I don't recall all of the details, but it was intended where we were kind of a big brother to them to help them gain a bit of a critical mass and direction. And it worked, I believe, because every one of the places where we had that relationship developed a more sizeable presence in the field to the point where about five or six years ago we discontinued it because there wasn't a need for it anymore and it had largely gone moribund.

As I look now at other centers, CMU has a little connection with the Heinz School, their policy school. Georgia Tech has some connection with the Nunn Center, there, with their policy. But none of them have the kind of breadth that we have across multiple disciplines, and I think that makes us unique in terms of the kinds of things we look at.

Yost: Looking at the list on your website it's almost 100 affiliated faculty, I believe, or at least . . .

Spafford: Ninety.

Yost: Ninety.

Spafford: And 90 from 18 departments, and the department designation is largely arbitrary. For instance, Jackie Rees and Karthik Kannan over in management got their degrees from computer science programs, and they're over in the management school. That's just the way that they chose to go. ECE is computer scientists, and more than narrow electrical engineers, and so on. The topics are more closely aligned than it would seem from the departmental boundaries.

Yost: Are there many social scientists that are working on privacy or other aspects of security research who are associated with the center?

Spafford: We've probably got a good eight or nine. The difficulty there is, again, getting support for them to do research in this area is very difficult because the need is still so intense to solve the technical issues, and that's where the funding goes, that there isn't a lot left over for some of the social sciences although there's more that is appearing, it's beginning to grow in that area. I hope to see a lot more.

Yost: Do you mind if we take a short break?

Spafford: Not a problem, I could use a break as well.

[BREAK]

Yost: Can you tell me about the start of the seminar and how that's evolved? And to what degree has industry participated, to what degree have academic researchers participated?

Spafford: Back in the 1991-92 timeframe, maybe, I think that's about right. One of my grad students spent the summer at Xerox Labs and told about a tradition they had there about getting together once a week and everybody had a five-minute around the table discussion of what they were working on. Well, this was at the time I had the DARPA money and a few other grants, so there were about 12, 15 students in the COAST lab. I thought this was a great idea because while they were working on different projects they didn't get to communicate with each other often. So what we'd do is we'd have one evening, one dinner time, because classes got in the way during the day, where we would order out — we'd get pizza or Kentucky Fried Chicken or Subway sandwiches or something — and while we were having a quick dinner we'd go around the table and people would present on things.

Well, this went on for a couple months, for not a long time, maybe two months. What we quickly discovered was that the majority of people, their reports were usually "I had a big project and the pilot's this week so I didn't get anything done", or "I ended up writing the whole front end because I was supposed to do it" kind of thing. And it was sort of interesting and helped get people in touch, but also it didn't quite get to the issue of learning deeper issues. So the next implementation I said okay, what I'm going to do is

I'm going to ask each one of you, one after another, to pick a topic that's interesting to you that we don't cover in class, and talk about it to the rest of the group.

So the student who was at Xerox, Christoph Schuba, — he's head of network security strategy at Ericsson now — was the first one. As I recall, he talked about perceptions of risk, which is something that came back repeatedly as a topic, and I have done work on it the last couple of years. So he gave a really interesting talk, and the next week was software forensics or something. But I had a couple students and a faculty member [say], I heard you had this talk on risk perception. I'd love to hear that, could you open it up? Alrighty then. So we'll offer that as another evening lecture only this time we advertise it around several departments.

Quite a few people showed up and interacted and had a great time. When are you going to do this again? Okay. Assign one of the other students to give a talk, similarly well attended. Hmm. Now there's obviously a demand for this, what are we going to do? So I set it up as a regular occurrence that after, I think it was before dinner at that point, we had it on the schedule, people would sign up to do a talk, and all the students we had in the lab thought this was great and they picked topics that they were going to do. And that worked well for the first year or so.

And then, the next thing that occurred is we'd be having visitors who would come to see us for one reason or another, and we asked if they'd like to talk in this series. So they would do that. The third year in, we — hmmm — you know, finding a room every week is a pain in the butt. If we schedule this as a pass/fail class we'll have the room automatically scheduled for us. So we did that and I started setting aside a little bit of money so that I could bring in speakers from outside because now it was a class and we needed to fill the sessions.

I started inviting people, and in particular, I would look for people that I knew who might be in Chicago, or Indianapolis, or Ohio; it'd be a short trip for them to come in. I started particularly looking for people with an industry point of view. I was looking for women, looking for minorities, because we didn't have a lot of those people in the program. We still don't. They're badly underrepresented in the field. I thought getting some different kinds of perception of the field for our students would be a good thing.

For a while, we had people who would volunteer. They would cover all their costs to come out and speak because they wanted to. And I started talking to some of the industry partners that we had and said you know, this is a really good way to get your company in front of the students. Don't advertise, come out and talk technical. And so they started supplying speakers.

Sometime around 2005 or 2004, Purdue has a distance education studio and we started using that. We started livecasting the talks on campus, and recording them and making them available online. As the technology's improved, we've improved that process. But we're now at the point, I think, where we have over 500 recorded talks that are available online for free; plus there were a whole bunch before that that we didn't record. It continues along as a weekly class. We invite people locally who have something they want to talk about. We try to get, in particular, some of the Ph.D. students, they use it as a practice for their defenses or conference talks; but we also invite colleagues from other universities, people from companies, people from government agencies. And most of them are all really happy to come in, give a talk, meet with the students.

We've discovered that the seminar series has been used as class material at universities, colleges, companies around the world now for years. We've had students show up who say oh yes, I took a class last year that every week we had the seminar, then we talked about it. A student from Madagascar came and told me that and I thought well, that's really interesting. Based on the numbers we have, we think it's the most widely viewed security podcast in terms of number of views. A number of companies every week download it and send it out over their internal networks to all their employees. Northrop Grumman has done that, Lockheed Martin and Nokia too. So it's turned out to be a good experience, but finding new speakers can be somewhat of a chore.

Yost: Has it helped further build and enhance relationships with various companies that have supported the seminar?

Spafford: It has. We've been able to get deeper connections inside some of the companies. We've invited people in that we might've not otherwise contacted, and they get to see some of what's going on here. Some international connections have gotten improved. It's been pretty valuable. It's also a great way to get colleagues in from other places to talk and see what's going on, and possibly generate some new connections. That's the biggest challenge I have, generally, is just getting the communication internally to be something reasonable, to get people to collaborate more. It's tough, the way that we're structured.

Yost: One area that you mentioned toward the end of last session that I'd like to follow up on is curriculum development. Can you talk about that in the computer security field and the role that you and CERIAS has had?

Spafford: There's a couple of different levels of that, and so there's the K-12, there's the college level, and then there's also degree formation; so I'll talk about all three of those.

Yost: Great.

Spafford: At the K-12 level, one of the first hires in 1999 that I made was for K-12 outreach. Going with a strategic vision of how do we increase the number of people in the field, we wanted to produce materials that could be used in curriculum and instruction at a K-12 level, and we have a big college of education here. We produce teachers for throughout the Midwest, so I had a professional educator, professional K-12 person who was doing development of that material. We produced some really interesting things, I think. Some of it was material that could be taught at a junior high level or high school level, about staying safe online and the like, or respecting intellectual property.

The place we got the most traction was doing outreach with K-12 teachers in school districts. Not necessarily providing material but in-service teaching and making them aware of what the problems were and what was involved. We produced a set of videotapes, in fact, that were very widely used around the Midwest and educational materials for teachers for continuing education credit for themselves, but teaching them about these issues that they used.

When the Lilly money ran out, we weren't able to do much more with the K-12. We had a little bit of money that we got through the Department of Education, hired an educational designer, produced some nice exams and some other materials that several places used, but then we could never get any follow-on funding. So when the senior person finished her degree and got an offer to go elsewhere, I couldn't make a counter offer, I didn't have anything. And the educational designer that we had, who had been a high school teacher for several years, got an interesting offer from his father-in-law to become general manager of their pub and it's become a major institution here in the community. He's done a very good job of it; it's an authentic Irish pub, he's happy, and we love visiting. But that was the end of our K-12 efforts.

I'll say at the graduate level, in 2000, shortly after the center was formed — Institute — there was no computer security degree in existence anywhere. There was no cyber security degree. Most of the students that we had going through, if they wanted to do that, basically had to go through the CS department. But that's a lot of very technical material and didn't cover the other elements that we wanted to cover — human factors, policy, security, economics. So several of us — Victor Raskin, senior faculty member here, Distinguished Professor, being one of the primary architects of this — he and Melissa Dark, and I, and Mike Atallah, and a few others created an interdisciplinary graduate program that has a core. It requires a strong slug of CS or equivalent, security classes and cryptography, and with their prerequisites, so about half the degree is purely technical. But it also requires a course in technology policy, and a course in technology ethics, plus a core sequence in what they're going to specialize in, whether it's economics or policy or whatever:, an elective choice. We got that approved in 2000 and we have been offering it to students ever since. We don't offer it a lot because if students want to do a master's in the technology, then they should go to CS or Computer Technology. But we've graduated Ph.D. students on a regular basis now. Starting in, I think, 2004 or 2005, Iowa State offered a degree. I think CMU offers one, RIT, [and] Georgia Tech now, but we had it back in 2000.

At the undergraduate level, we struggled with this for a while, and we're still working in this area. Melissa Dark, who I mentioned is now over at technology as a chaired professor, continues to try to push on aspects of this, setting up programs and curriculum. I was involved and am off and on, and I'm again involved in it with various groups about what should be in standards, what should be in curriculum; the Center of Academic Excellence is sort of a part of that.

I've actually been working in this area since 1988, when I got involved with ACM/IEEE curriculum effort. The curriculum output of that effort, the 1989 curriculum effort, included for the first time recommendations for course units in security and ethics, and that was my doing. So it was fortuitous I was involved at that point and it's grown every year since in the ACM/IEEE recommendations and CSAB/ABET requirements.

But we met with folks at NSF. We met with faculty at several of these other institutions to try to talk about what should be in a curriculum, how should it be introduced. Several of my students have gone on and worked in this area because I had them involved in this concern. The general premise that I've had all along is that the majority of specialization work in security is more graduate-oriented, — that an undergraduate really doesn't even have enough time to understand how computers work. They need to have a strong grounding in that if they're going to work on the technology of that. Or if it's policy, they really need to have a strong grounding in policy, plus technology. And the aspects of the security are really an add-on once you have the basics, but there are things that could be included in the base. So you should never teach operating systems without including some modules on protection in operating systems. It's fundamental. Or database and protection, and so on.

There's a long list of things that I probably could reconstruct, of meetings I've been to where I've talked about this, where I testified in front of Congress about it, or met with NSF or OSTP, but I'm not sure that I can point to any one thing and say that's a direct result of what I did. I know that a lot of these efforts, at some point, I may have had my fingers in, but it's an area that's still evolving.

I mean, just yesterday — there's a program that's starting named National Centers of Excellence in Cyber Operations. I have some deep doubts I raised to the parties involved about what they're teaching, when they're teaching it, how they're teaching it. We had a long discussion, and I think they will modify it a bit based on what I said.

This continues to be an interest of mine because working with the students is one of the things that gives me the greatest pleasure. So I don't know if I answered your question.

Yost: There's obviously a great need in the federal government for computer security professionals and a number of people are being educated at places like Naval Postgraduate. Are there fundamental differences between the computer security education at institutions such as that versus places like Purdue and Carnegie Mellon?

Spafford: Oh yes. Well, every educational institution has a somewhat different character as to what they try to do. Ours is strongly influenced by being a land-grant university with a tier one research profile. So our students who go through have a strong sense of building defenses, working in networks, and research orientation, all in service to the public.

Places like NPS and AFIT [Air Force Institute of Technology], as defense oriented universities, are actually — they have a lot more on intelligence and cyber operations than we do. There are other places like Tulsa, where they're very strongly allied with law enforcement and do a great deal more in forensics than we do. So there are differences in character.

One of the biggest differences in philosophy is that there are a lot of people who believe that the only way you can protect a system is to know how to break into it and I really, firmly reject that. That is a way to gain some knowledge, but it is not the way to learn how to defend, or even defend best, and I challenge anyone to show peer reviewed figures otherwise.

We produce students who are very good at defending a system and we don't teach them how to break into things, we don't teach them how to write viruses or the like. Lots of schools that do teach much more hands-on oriented, even down to the community college level it's very hands-on; here's how you configure this, here's how you run that. It is very different from what we do because we do a higher level research–oriented degree. We include policy. We include human factors. We try to present a broader view than defending against a particular threat. It's actually understanding the context of security.

Also, as I noted earlier, our land-grant heritage is to do things in the open, for the good of the public. We don't have a tradition of running off to do a start-up for every idea we have. Instead, we publish, we share code. Some people think that is stupid, but it's a values thing, and it permeates a lot of what we do.

Yost: One area that you brought up that we don't have much content on in any of the past interviews we've done is security economics. Can you talk about that subject and who do you see as some of the leading figures that contributed scholarship in this area?

Spafford: Ross Anderson, Joan Feigenbaum, come to mind for me right away; Ross is at Cambridge and Joan, I think, is at NYU. But I don't follow that area closely.

Yost: Is that Ed Feigenbaum's daughter?

Spafford: I think so. And I'm trying to think of the guy out at Berkeley who started their interdisciplinary program; an economist, and I'm totally spacing on his name. [Hal Varian] Well, Berkeley has an interdisciplinary school that includes some security people in it, and lawyer. Pam Samuelson is part of that. I'm just totally blanking on his name, but the economist who started that has also done work in this area.

From a practicing side, there are a lot of questions about how organizations view the risk and are willing to fund the research necessary to fix this. One of the biggest problems, I believe, in our current infrastructure is people just don't want to pay for security. They view it as a cost center, and so the return on investment is not measureable, there's no data for it. It really has to be viewed as a preventative, as a cost of doing business, really. And we don’t have the measures for that; we don’t have good history for the values. Many organizations would be better off if they’d junk all their legacy stuff and started over with better designs. But that represents a write-down of very often huge investments. Companies producing software or hardware for a very long time did not see the value in getting all the bugs out or getting the security right before they released it. All of this is economically driven, it’s not technology; we understand technologies. Even if the technologies were free it would still take time to execute and that’s an economic cost. So there’s a lot of work that could be done with what we know now. There’s a lot more that needs to be done here. I think economics is one of the issues that hinders us. There’s also an issue having to do with funding of work in the area, funding of research of students, and so on.

From an industry point of view, there’s a tragedy of the commons issue here that for companies to spend a lot of money on this over a long period of time just doesn’t make sense if they’re the only ones. That was part of what went into my design of the center here. We don’t charge up front a lot of money to be part of the effort.

Commons problems really fall to government, and this is typically a role of government, is to fund those things that do get into this category. Again, without a really clear threat and losses, it’s difficult to get money in a political system. But all along, it’s fairly clear, there has been an existing huge emphasis on offensive capabilities and exploit[ing] capabilities for intelligence. There’s probably at least an order of a hundred magnitude difference between the funding for offensive and for defensive in the field. Investigation gets almost nothing. Up until a few years ago, when I stopped looking, the entire budget for NIJ for cyber forensics technologies was $5 million a year for the whole country, the whole year. It's just no money, basically. Even if they made it $50 million, it's still way under anything else that's being done. So the economics of this is a complicating factor, even at the low level of government funding.

Yost: Do you see NSF's Trustworthy Computing Program as a positive force?

Spafford: It's positive but way underfunded.

Yost: It's what, about $50 or $60 million?

Spafford: Thereabouts. Of the people who still try to submit to it — because a lot of people no longer even try to submit; I know, because I talk to them — maybe one out of eight is successful. So it's a huge time sink to write a proposal, for odds like that of success. It's very discouraging for faculty. Last I looked, the majority of people who seem to write for that program are junior faculty, not senior faculty. It isn't worth the time for the senior faculty to do so.

Yost: Are they seeking money more from industry or where?

Spafford: Other agencies, and industry, yes.

Yost: And what principle agencies?

Spafford: DARPA, some; IARPA, some; DOE, ONR, AFOSR, ARO, sort of the usual suspects in that realm; DHS has funding but more for implementation than for basic research. I think those are probably the major ones. There are a lot of other spot programs that somebody who knows somebody who knows somebody who knows somebody, occasionally, there's some funding that comes about.

Yost: I've been doing some research with some interviews and trying to gather some other materials on the origins of the computer security industry, and I just want to get your perspective on some early developments out of the 1974 SHARE meeting. An outgrowth of that was RACF and Barry Schrager's ACF2, and then shortly thereafter, Top Secret. What is your view of what those products accomplished and failed to accomplish?

Spafford: Those products specifically?

Yost: Yes, well, more broadly, commercial access control security software products in the early days.

Spafford: I don't have personal experience with the products; all I can say anecdotally, what I heard from people is that they became compliance check box solutions. People would check yes, they do have RACF, but it would still be in the box on the shelf. It wasn’t deployed. But, as I said, that’s anecdotal and I can’t tell you beyond that because they’re not systems that I used.

Yost: And any perspective on Trusted Information Systems as what appears to be the first sizeable services contractor in security?

Spafford: Well, TIS was started by a security person and was in direct response to needs there, so it certainly made a splash. You saw things that came out of there like really the first firewall was something that they produced. At the time that they got started, there were changes going on in the field as to the kinds of computing being done, networks were becoming much more common, Unix-based systems, minicomputers rather than mainframes, and this changed a lot of the sense of what was needed for security.

This part of the whole trend that I was talking about, practical security, the idea of how do you fix the things you have rather than holding out the Orange Book and saying we want you to build this. We have these systems, how do we make them better? That’s been a driving force through much of my career — is not pull out a Holy Grail and please do this, and not necessarily saying, I’ve got this thing from lowest cost bidder now how do I make it impervious, — but advocate a middle ground.

And I had this experience, I think it was in 1993, 1994; I can date it in the sense; I think it was 1993. No, it was 1994, I remember now, it was spring of 1994. Spring of 1994, a report came out from something called the Joint Commission. It was “Re-evaluating Security” was the name of it, and they recommended going from an all-or-nothing model that had been done with computing security, to a risk-based model, which was a real departure from what had been done.

I remember, right about the time that came out, in that spring of 1994, I was invited to give a talk at a CIA location in the general Herndon, Virginia area. I don't even remember where it is now; it was off the road to the airport. And they got me badged in, and were showing me around their data processing center, and they informed me that they had gotten special permission to show me something really groundbreaking. Wonderful. So we went through this controlled access door with armed guards on either side of the door, walk into this rather vanilla computing room that had one machine running in the center. It was a big Sun server machine, and there was nothing else in the room. I said, this machine is historic? They told me it was the first network connection between — hope I get this right — I think it was IntelLink and JWICS or SIPRNet. I don't remember which one of those networks, but it was IntelLink, which was CIAs intelligence network, and some other network that had client types on it at a high level — probably JWICS and IntelLink. Wow! I mean, this is a big deal to connect these two networks together because the CIA really protected their networks.

It was on a Sun running Solaris or Sun OS, actually, and I said wow, that's really impressive. They said "Oh yes, we went through all kinds of design; we have state-of-the-art security running on this system." That's interesting. What's state-of-the-art? "We have two of the top software programs in the industry, we have Tripwire and we have COPS running on it." The feeling of distress I had at that point was really palpable, that two summer projects by my undergrads were viewed as state-of-the-art security, guarding the CIA's network from intrusion.

Yost: Did they know that you were the origin?

Spafford: No they did not. They had no idea where those came from. And the sinking feeling, just the terrible feeling that I had about this as the state-of-the-art; I mean, I'm proud of my students, I'm proud of *all* my students and all the things they do, but what they build as students are clearly not the industrial strength kind of things that needed to be done here. I started looking more at what was available in the commercial marketplace, and there really wasn't a lot at the time. That was one of the reasons why I didn't try more to commercialize what I produced; it was a very different era, that's why I didn't seek patents on the things that I did or do startup companies because there wasn't a business there. Instead, I wanted to release things that just made the environment better and show people what could be done.

I've often thought about well gosh, if I had gotten patents on everything or tried to build companies, how would life have been different? So, for instance, after COPS was released, about three years after COPS, four years after COPS, the guys who developed ISS developed that as a program and started selling it. They didn't have a big market at first, but we were kind of well, look at what they're doing. If we'd sold COPS I wonder if anybody would've even bought it at the time. Of course, ISS went on to become a very major product.

The marketplace — and this is part of the economics issue from earlier — just really didn't exist much in the early 1990s for this kind of thing. It was word of mouth. It was a community of practitioners that we built a lot of homebrewed things and we installed them. There was not a lot worth paying money for.

Yost: What is your perspective on the CISSP credential and the impact it has or hasn't had?

Spafford: So there's a little history there, when the group got together to form that certification [CISSP], because they were trying to standardize — legitimize is the wrong word, I'm not sure what the right word is — but to really establish that it was a certification. I knew most of the people on the board. They asked me to provide some input, which I did. They came up with the idea of the test and the initial body of knowledge, a little bit of which I contributed, and they wanted to field test it. So they arranged for a couple universities around the country to field test against their students. We had it here on a Saturday. It was a multiple choice test, and they asked me to identify some students. I think I found 20 of my grad students that yes, they'd spend a Saturday and take the test. And apparently they, both collectively and individually, blew everybody else out of the water, including the pros who had been out in the field for a while, which I felt good about. We had the highest group score, and we had the highest individual scores, and our lowest scoring person scored higher than the highest person at any other university. So that felt good, to know that we were teaching the kinds of things that were viewed as important, but it also said to me that this was an exam that if you studied, if you were in a class where you didn't have practical experience, you could pass the test. And so it cast a little bit of doubt for me early on, as to whether it was really measuring what they wanted to measure and I was very vocal about this.

One of the things, in fact, I was vocal about was that people like Matt Bishop and Dorothy Denning and myself could not qualify for a CISSP because they didn't count the kind of experience that we had as experience. That didn't seem right, somehow, considering that all the sit-down tests were based on material that we taught and out of books that we wrote. It wasn't quite clear what it was that they were actually trying to measure.

You've talked to Bill Murray, and he was one of the movers and shakers on this and he probably has a better perspective than I do. But what I saw is they modified the requirements of what went into certifying someone so that now there is a proof of experience, a proof of work, along with the test. It is not ideal but of all of the certifications out there, it is probably one of the best to at least show that there is awareness of basic concepts. Like a lot of other tests, it's possible to cram for it but even the act of cramming is likely to help; I don't think a total novice is going to be able to do well on it. So overall, I think it's a reasonable approach. It doesn't come anywhere close to getting a degree or otherwise, but of all the various certifications that are out there I think it's one of the more meaningful ones.

Yost: Can you tell me about the history of the journal *Computers & Security*, and how it evolved, and the directions you tried to push the journal in when you became the editor-in-chief?

Spafford: In my other office, I have the journal going back to the very first issue. When Harold Highland died his wife gave me his collection, so I have a complete collection of paper copies of the journal. It goes back 30 or so years, as I recall. Harold started it, along with a group of practitioners who wanted an outlet to discuss trends and talk about discoveries. So it was almost a newsletter or magazine kind of document at first, the first year or so.

As the field grew, they began to get more contributions of a more scholarly nature, and I don't remember at what point it occurred, but IFIPS Technical Committee 11, there was an alliance formed, so it became the official outlet for TC-11. And when that happened they had a research community and conferences to use it as an outlet.

Harold was the editor for a very long time and spent time soliciting articles from young people. He had a very definite vision. He had a large section where he had news and happenings in the field; things that people may have missed in other media. This is really before a lot of what we have on the Internet today, so he took that approach and it was really valuable.

When Harold died, Jon David, a friend of Harold's, was the interim editor. I'm trying to remember who was next; Bill Hickcox? Gosh, that's terrible, I can't remember his name; a real larger than life kind of guy, bombastic. Made a number of claims I believe were shown to be false about his background as working for special operations, and all kinds of things, but he was quite a character. He was editor for a short while and then died suddenly. Then Gene Schultz was editor for a while, and he unfortunately passed away two years ago. Steve Wolthausen was editor for a short while, and then me.

I’ve been involved with the journal since the time of Harold’s death. I was a reviewer. I was involved when Harold died, I was approached about being the editor at that time, and that was probably 1998, but I didn’t really believe I was ready to do that. I had too many other things going on; I didn’t have enough experience. But I did accept a position as the academic editor, basically the associate editor of the journal, and I kept that position up until I became editor-in-chief.

The journal has evolved over time as other journals have come along, other conferences and journals, they’ve proven to be outlets for information. ACM and IEEE, in particular, have some very well-respected journals that draw from an awful lot of North American authors. But *Computers & Security* is still pretty much the journal for the rest of the world. People from the U.S. and Canada do publish in it and provide the majority of articles, if you look — well, not the majority — the country that provides the most articles is still the U.S. but the majority of the articles are elsewhere in the world. TC-11 continues to have it as their official venue and their newsletter.

The model while Harold and Jon were editors, and a little bit Bill, was articles for the practitioner, scholarly articles for the practitioner, things that they could immediately use and put into play. It then began a drift towards more theoretical and academic articles, especially as the Internet became more the medium of immediate news. When I took over as editor, there were some obvious problems.

Actually, before I took over as editor I got the publisher to change, to stop accepting articles on cryptography. Cryptography articles are definitely within the scope of security, or cryptography is, but the problem is that you have lots of people who think they’re cryptographers, it’s easy to write a new algorithm or a new problem, and it’s an extraordinarily long time to review it well, and requires a skill set that isn't common. So not everybody can review cryptography articles and the journal was just getting a huge backlog of cryptographic related stuff, much of it was coming out of China and India, and where nearly every article was being rejected when it was finally reviewed, but it was clogging up the system. So the journal doesn't accept those anymore.

When I took over the journal, there had been a backlog of articles and there was a bit of a downturn in submissions. The acting editor, Dimitris Gritzalis, had done a great job reducing a huge backlog, but that was not a sustainable process. My goal was to keep the review cycle short. People have gone to publishing at conferences and treating that as important because the turnaround with journals was so slow; sometimes it'd take two years to get a review. I've gotten it down on *Computers & Security* so that the average review cycle from submission to first response is under eight weeks. And the average time from submission to online publication, an article, if it's accepted, is a little over eight months. That's a really good turnaround time and I continue to push on that as much as I can with the editorial board we have.

I'm trying to solicit things like book reviews and invited essays to get a little bit more than just what people want to submit, but trying to find some topics that people want to use. And working with the publisher to try to find ways to make it more accessible cost wise, and content wise. That's tough because Elsevier is a commercial publisher and their model doesn't support that but I think that's important for the future of the journal. I'm also trying to get TC-11 to be a little bit more active in what they provide. That's difficult but I'm going to continue pushing on it.

Yost: You've received many honors, and most recently, the Hall of Fame. Can you talk about what those have meant to you and your perspective on that?

Spafford: Yes, I've gotten a few things.

Yost: [Laughs.] Yes, the wall is covered awards and certificates of appreciation.

Spafford: They all mean something to me. They don't all mean the same thing. For a lot of my career — there's a placard in my other office that's a quote of Mark Twain about "always do right, it will gratify some and surprise the rest." Mike Atallah, the person I first told this to — when I was an assistant professor, a green assistant professor — I told him, I'm going to do what I think needs to be done and if that gets me tenure, great, and if not, well I'll go somewhere else. That has been my philosophy all along. Both are expressions of the same thing.

I'm here because I see that there are things that can be done to make a difference. I really enjoy working with students and helping them realize some potential and go out and do things. I am not the kind of person that would fit at a CMU or an M.I.T., necessarily. I could, if I really wanted to reorient my world. I don't sit down and write lots of papers. I wouldn't fit out in California. I'm not interested in starting companies, which seems to be Stanford or Berkeley — get an idea, write a paper, and then go start a company — I'm not in those categories. As I mentioned, I don't go to the IEEE conference. I don't have a huge list of things that have appeared in *IEEE Transactions*, that's not the audience that I've primarily been focused on. So some of these awards from some of these organizations have meaning to me because they say that even though I've taken a somewhat unconventional path — not quite the path that others would expect — it is valued by the academic community or by the practitioner community. And that means something to me that it is valuable, it's viewed as valued. That isn't to downplay the work that I have done, that has been published in some of the better venues. It simply is that my definition of success is more about how I can improve the world than in how many publications I rack up or how much money I make, and apparently some groups appreciate that, too.

The teaching awards mean a lot to me but some of the best rewards are occasionally just getting an e-mail from people that I don't even remember who say that a class I taught was important to them; that's a wonderful thought. When I started down this path, I realized no matter what I did, I would probably never have a theorem named after me, or an algorithm. I was not going to be a contender for a Turing Award or the NAE, and that was just fine. The way that I've always felt that I'd influence the future is by setting an example for others and by teaching others to go out and make a difference. I'm the stone, they're the ripples, as it were. The stone sinks quickly below the surface but the ripples go on for a while. So if I have, along the way, been able to inspire others or to inspire some of their lines of research, great. I've started a number of things that other people have picked up on. Some they haven't picked up on, some it takes a decade or so to pick up on, that's fine.

What I've been trying to do over the last decade is to pick out individuals who have been making a difference that I haven't seen them getting the same recognition, and then trying to push them forward to get them recognized for the things they've done as well.

In large part, what these various recognitions are about, some are thank yous, I suppose; some are to collect people together, to inspire others to say here's something that you can aspire to. I really believe that for some of these — Hall of Fame, for instance — great bunch of people but others can aspire to be part of that, we're not that different. One or two these recognitions may have been given to say "Enough already." I like to think that's not the case because I don't think I'm done yet.

I guess that's what they mean to me. I don't know what else to say about it unless there's a particular one you have in mind.

Yost: What are your goals for CERIAS and how it evolves to the future, and how it connects in its future needs?

Spafford: One of the reasons it has a name, CERIAS, is to be independent of any one idea or person, and it was generic enough it could encompass a lot of different ideas. My goal has always been to build something that will continue after I stop. I'm not as confident about that occurring as I would like to be, in part because of where it fits into the university structure, the university mission, makes it very difficult to make something like this work. It takes several individuals, not just me, but it takes several of us, quite a bit of effort to keep the momentum going. I think we've already fallen behind in several areas where we had the lead and we could've done more, such as innovative education. It's terribly, terribly difficult to get new courses introduced that would be supportive of what needs to be done because it's not a priority of any department. We're not a department and in fact, we’re at the mercy of department leaders who develop strange ideas about what they want their department to be.

So as I look forward, I really would like to see this perhaps transition into an academic department. Purdue’s the place where the first CS department got started and I don’t see why we can’t do something like that for security and privacy. We wouldn’t be the first, there are other places that have done that but I think we can do it a different way to embody this multidisciplinarity. I haven’t thought about it a lot beyond that because if it does continue and if it does grow as an organic thing, it’s got to do that based on participation.

I can certainly see directions where things could occur. I’d like to see, for instance, companies have more of a local presence and involvement with whatever entity is going here. We’ve got three offices in our technology park that have been opened by our technology partners just to be closer to work with us. We are a little bit remote from where they are headquartered. I’d like to see more of that occur. I’d like to see maybe a few more startups come out of the center.

But most of all, I’d like to see a set of coordinated resources and recognition to carry this mission forward. But that’s really going to depend on the people involved. I can take it so far, and if it’s going to continue it’s got to be done by those that follow on, and that’s probably the biggest concern.

When I started here, I had two publications — not a lot by today’s standards — I had good letters, I had done a lot of work, but also looking back at my background, as an undergraduate, during the course of my career I think I had seven different academic majors before I finally picked two. I did two minors as a grad student. When I showed up here, I was still a master instructor for the Red Cross, I was still teaching classes for them. I'm not exactly focused on one area alone. I see things as systems; I see things in ways others don't. That may be part of my success. It's certainly part of the challenge in dealing with different departments, different cultures, different mindsets, to try to see things their way and get them to work together. That's a huge challenge here. But the current environment tends to breed out individuals like me. Having a range of interests is no longer as legitimate as it once was; the academy doesn't want polymaths. One has to have a very narrow focused view, and be world class in that view rather than very good in several to succeed.

There may be a certain element of blind spot, a certain element of hubris here: I don't see anybody like me coming up through the ranks. I don't see anybody else who's got that kind of broadly-based view, and that worries me. I wish our community and society had a broader definition of success.

But that's related, too, to something I said earlier. I can't get an audience with senior people in government or industry because I am not "successful." What does that mean to them? I haven't started a multi-million dollar company. I haven't risen to the rank of university president. In their value systems, I'm a failure because I have not achieved what they view as success. And many of the people who have had that "success" have no real idea what they're talking about in this space.

Based on the work I've done, I've gotten courtesy appointments in five academic departments. We have a few people who have a courtesy appointment in only one and it's not often clear why they have it. So the thing that worries me most going forward about CERIAS or anything else is where do we find the leadership, the one or two people to do that? Or what is the transformation that would allow somebody who's currently around to lead it. I don't expect to find a duplicate of me, okay? That's fine, but what do we do to do this.

If that doesn't happen, if for some reason the root university mission or whatever else causes CERIAS to evaporate, I think that'd be a little sad but not tragic. We've had a 16-year run so far, and I intend to continue doing this for a few years more. And I think my colleagues and I and our students have made a transformation of the landscape in the field that's pretty close to what we set out to do in our original strategic plan. The original strategic plan was to increase awareness, increase research, increase the population, and we've done that. So I don't feel in any way that a discontinuation is tragic — I think it would be unfortunate. I think there's an amount of good will and recognition and organization that could continue to do more. But if I had to walk away from Purdue tomorrow, I'd miss it, but I wouldn't in any sense feel that there's something major that hasn't been accomplished yet,— that has been nagging me to do and I would regret forever. Instead, I'm happy with what I've done — I'm not content or believe that I'm finished — but I'm happy with what I've done.

Yost: Finally, are there some topics I haven't covered that you'd like to discuss or areas that I've brought up that you'd like to say more about?

Spafford: Probably. I've had a couple fleeting thoughts while we were talking but I didn't note them down. So let me suggest taking a short break. I'm going to go get some coffee; I'll wander down the hall. You can as well, if you're interested and then I'll come back and address that.

[BREAK]

Yost: So you have come up with a handful of additional topics or areas to expand upon could you begin with them in order, so your parents, family life, and growing up?

Spafford: So, one of the things about who I am — I am sure it is partly attributable to my upbringing. I have a younger sister younger by two years; sort of traditional family. I'll say a few words there.

My father was born in 1918, right after the first World War, lived through the Great Depression, got a degree in college, enlisted in the military in World War II, served in World War II; worked very hard all his life. And my mother was born shortly after World War I, her father died when she was 14 from injuries sustained in World War I. She also lived through the Depression. Very core values.

I was born in Rochester, raised in New York state for the first 21 years. Issues of fairness and honesty were clearly evident throughout our lives. We had very little money as a family, so I'm quite comfortable on the salary of a university professor. I don't feel the need to go out and start companies, because I realize how much value there is, really, in people around me, not in things. And all of that has helped influence me.

As a youngster in grade school and high school, I was always different than the rest. I did catch on to things better; the math and the science, I just loved it. Early on, as a child, my parents bought a World Book encyclopedia as a reference for me for school and I actually sat down and read it from cover to cover, the whole set. It took me well over a year, but I loved it. I've always enjoyed learning about things.

I also had some physical problems. I have bad vision, I've had joint problems my whole life, and so I wasn't able to really participate on sports teams or anything like that, it's just not my nature. Although I did end up as the student manager of the football team and the wrestling team, and actually got letters for my participation in that, which is not great shakes but I was accepted, eventually, some.

Usually, I got a lot of taunting, a lot of picking on. I never got beat up but intimated a lot throughout school by people who wanted help with their homework, who were making fun of me because of intellect or how I dressed, those kind of things. Didn't let it bother me a lot but it did hurt. I was never a "cool kid." Or adult.

Like a lot of people in that situation, I learned to develop a sense of humor, which I'll come back to. But throughout it all, there was this underlying sense of right and wrong, and what should be done and what should not. It was family, it was community. Maybe some is genetic?

That was a natural view for me as an undergraduate, why philosophy was one of my minors, and courses that I liked. And in a wonderful bit of irony, I had a 4.0 average through my undergraduate degree with a double major, until my last semester when I ended up getting a "B" in ethics because I argued with the professor. I disagreed with the professor about some of his statements about right and wrong. I challenged him in class. He didn't like that. I didn't care. But that's been something central to a lot of my career, is I'm in this area because it's a matter of doing the right thing, of getting systems to do the right thing, of being trustworthy, and I impress on my students that is really the core of our program.

That's another thing that differentiates us at CERIAS a little bit — I try to permeate all that I do…. I mean, behind you I have the ACM Code of Ethics up there and Professional Conduct. I require all students associated with CERIAS to complete the CITI program online on research, responsible conduct of research, professional ethics. Hold everybody to a good standard of treating others fairly. I don't see as much of that going on in the field as I would like. I think that for us to build trustworthy systems we have to be trustworthy ourselves and we have to hold ourselves to a higher standard as a profession. A lot of what goes on with penetrating systems and selling vulnerabilities, and the like, isn't setting as good an example as I think we should. Privacy's very important; we have to respect that more as a field than we do.

I don't want that to come off sounding holier-than-thou. I'm not perfect, and I can't claim that I have absolute insight into the truth. But I believe it is really important to keep thinking about those concepts, but not as an afterthought.

Yost: Is the fact that some former hackers have found lucrative positions, is that a problem as you see it?

Spafford: That's very troubling to me in some cases.

Yost: I think there's a number of people, former hackers, in computer security research, consulting, and practice.

Spafford: Certainly, some of us who are a little bit older, who perhaps — I mean, that's not entirely fair to say, but those are the people I know better — it troubles us and that's kind of the environment we were raised in where the issues of honor and trust are very important. The fact that people like Kevin Mitnick, as an example, being held up as an expert in cyber security, which he is not, and paid lots of money for speaking appearances for basically a history of criminal behavior is distressing. On the other hand, Robert Morris, who wrote the worm, …well, as in interviews that I've had recently on that, as I say, I think has displayed exemplary behavior on this. He hasn't profited off this, he hasn't bragged about it. He doesn't advertise it. He stopped working in the area. He really appears to be contrite and reformed on this.

So it's not that I believe people with bad behavior should never be trusted again, but I think it's wrong that bad behavior is rewarded. That's a very strong element that runs through a lot of what I do. One of my early papers on the ethics of hacking — that wasn't quite the name, I don't remember exactly what it is, now, but it was some time ago — has been very widely printed in ethics books and is very widely cited. Some of the people in the philosophy department knew who I was and had no idea I did security, and that was my first courtesy appointment here was through the philosophy department, so there's that topic.

Yost: And can you discuss ACM?

Spafford: I joined ACM as a member in 1978. They didn't have student member classes back then, it was you were a member or you weren't. But as a regular member, you got to pay half dues if you were a full time student as I recall, so that's what I did. Six or seven years ago I became a life member, so I've been continuous for 35 years as a member of ACM. I've also been a member of IEEE and its Computer Society for that length of time. I've achieved fellow status in both.

ACM has been a better fit for my interests and some of the things that I've done. I've been fortunate that I got involved in the joint curriculum task force effort, and I was able to contribute there and that was wonderful. I became chair of the self assessment committee for a few years. I was involved with awards committees. And then I got appointed to a membership in the USACM Computers and Public Policy Committee, as it was named at the time.

When Barbara Simons became ACM president, she asked me to chair the committee, and then when she came back she was co-chair. But ever since Barbara ascended to the president I've been chair or co-chair of USACM for Public Policy, and this resonates a lot with both my sense of right and wrong and my interest in policy.

As I mentioned, at one point I thought I might be interested in law; maybe it wasn't law that I was interested in, it was more the public interest, the public affairs. This has helped scratch that itch a little bit and I've been involved in policy in a number of different initiatives here at the university and outside. So the USACM and other ACM activities — that isn't the only thing I've done with the ACM, I've done a number of other things — that's been a very prominent aspect, I think, of some of my activities, my persona, on the outside.

I’ve worked very, very hard with that group to bring them together to comment on issues without taking sides. The role of the USACM is to comment on policy issues without being partisan, to comment on the technology as we know it and about the role of the computing professional without trying to influence the legislation in a particular way. And that’s not always easy because we have people from all over the spectrum on nearly every issue. But it’s been great fun. It’s been rewarding. It’s led to me testifying before Congressional committees, on occasion. I’ve served on Presidential advisory committees, maybe not for USACM, but that maybe could be a part of why I was chosen. I’m going to an event in Washington in the next few days that came about because of my USACM connection.

USACM grown from a group of 12 people to nearly 100. It’s gone from being a committee of ACM to being a formal council of ACM. And the last few terms, I’ve wanted to step down but we haven’t found a good candidate. Now we have a good candidate — I’m not going to say who — but I’m definitively stepping down on June 30 as chair of USACM and becoming the past chair. But I’m also now a member at large in the ACM Council, and I will be running for the vice president’s position of ACM in the next election.

ACM embodies a lot of good things that I think are good about the profession. They promote scholarship, they promote education; very strong on some of the issues of values; inclusion, equality; a lot of the things that are beyond simply the intellectual content that make an area something worth being a part of. I don’t see as many other people recognizing, currently, the value of being a member of an association like that. I wish more did.

ACM isn't the only such organization, as I said, the Computer Society is also a very good group. The ISSA is a small organization that's getting started in information security. They've been around for decades but I mean, they're continuing to grow as another very good organization. But ACM has been probably the primary one for me.

As I mentioned, policy has been a big issue for me, and this goes with my sort of interdisciplinary view. We can build technology, but how we use it is the issue, and whether we use it is the issue. I can build a number of different kinds of artifacts and whether they're used for good things or bad things is really a human decision, a policy decision. So understanding what causes people to make those decisions and being sure that they have the right information and maybe shaping the technology so it's easier to use in one direction than another, are areas that continue to interest me. That's where a lot of my current research, recent research, has been, in understanding risk and forming policy. I'm currently doing some work on the role of deception in computing. These are all human thought processes rather than the technology and I'm finding those to be interesting and not well explored areas. So unless something else happens, I suspect the next five years, probably — not the final years of my career, but beginning to wind down — are going to be devoted to topics in those areas.

Yost: How do you view Peter Neumann's work done in the area of risk?

Spafford: Oh, it's really great. Peter's book was very valuable, still. It's one of two books in the area that — for a long time I taught an honors undergraduate class to try to keep students involved and that was one of the two books — Ritchie Epstein's, *The Case* *of the Killer Robot*, was the other one, which goes a lot to policy and ethics and responsibility. Peter is, as well as a collector and archivist of these kinds of issues, has served a tremendous role in the community. He maybe hasn't synthesized as much as some might, but simply the ongoing curation and people know that there's a place to go to find these issues, is really valuable. He's also contributed a huge amount as a research scientist, advisor, mentor. The only other person I've seen like that in the community is Dave Farber and his list. Peter got the Distinguished Service Award from the CRA last year, and it was very well deserved; he's done an awful lot for the community.

Yost: And the problems you've had with your hands?

Spafford: So not something that I talk a lot about, but I mentioned briefly that I had joint problems as a kid. I've had problems with my hands and arms my whole adult life. It has flared up from time to time and 1993-94 was particularly bad, I had to wear hand braces most of the time, awake or sleeping.

During much of a formative decade, from 1990-2000 and then a little bit beyond, I would have episodes where I couldn't type, couldn't respond to e-mail, couldn't produce papers, and had no good voice recognition technology. So a number of the things that I've worked on I've had to turn over to students and let them do papers on. My name doesn't appear on most of them. Or colleagues, I'd give colleagues ideas but couldn't help with the papers or the programming.

I still have problems with my hands. We may actually be narrowing in on a medical reason for why that is the case, awfully late to know that. And I still have bouts like that where people ask me to contribute to a paper or write a paper on a topic and I have to say I can't.

This has shaped, in part, some of what I do because I'm not able to produce the publications that are typical of an academic, because I can't. Over the last two decades I've probably done a lot more public speaking than most, because that's the way I'm able to get the ideas out. It doesn't reach as large an audience, it's not as effective. Someone like Bruce Schneier is writing essays every week that a lot of people read. I've had to develop more as a speaker because I can't do that writing, and with my luck, in about another five or six years, speech recognition will finally get good enough I can finally do papers that way. But it's one of those things that, well, it's interesting to think what could've been, but it's a matter of going forward with what I've got. I think that's kind of worth stating for the record that there were these periods of time when I just wasn't able to produce things.

There was one really difficult time when I was on the PITAC committee, the President's Information Technology Advisory Committee, and I also helped chair the CRA's Grand Research Challenges workshop, and I had a six-month period when I just couldn't type anything, and reports were needed for both. It was really terrible to be on a critical path and not be able to do anything really about it.

My kidneys have been damaged from taking too much Advil over the years to try to cope with it. Not badly enough that I'm in any kind of critical condition, but as time goes on that may lead to complications. I didn't know. And it didn't help, — anti-inflammatories didn't really make any difference.

There's a phrase that I've seen many times that we should be kind to everyone because each person is fighting at least one battle we don't see. Well, this has been one of mine that's been an ongoing issue, and it has given me great appreciation for that aphorism, and more toleration of others.

Yost: And the topic of "government."

Spafford: As I said, my father was a veteran. One grandfather died of injuries [suffered] in World War I. I've had a number of relatives that have been in military and government service. I think that is becoming less common with time — many of my colleagues and students don't know well anyone who has done that kind of work.

I generally believe that everyone I've met employed in government, almost, has been incredibly well intentioned, good character, cares about values. The collection, sometimes, takes some very weird directions, however, but the individuals are sound. And I won't say that all the elected representatives I've met are the best example of what we have in this country, but particularly when I go to I work with the folks in law enforcement and the military, the sacrifice, and the intellect, and the character is really significant.

When I was just a new associate professor, I got invited to participate in a special program called the Defense Science Study Group that DARPA funded through IDA. There is a section on my web page about that experience. It's been running for over two decades. Every other year, a small group of faculty, multi-disciplinary, are taken and given some in-depth exposure to what goes on in the Defense Department, simply so we can understand a little. They don’t want to turn people into fans, that’s not what they’re after, it’s more just to understand the problems and meet some of the people. And as a consequence of that, a lot of people who go through the program have more inclusive research or serve as advisors to government agencies. I was an advisor to the government before that occurred, but it reinforced a lot of my perceptions of people working in government and in the military.

One figure that was quoted to me is that nearly 90 percent of everybody at the rank of major in the military and above has at least one graduate degree. We have an incredibly well-educated military although not many in academia seem to understand that or appreciate it, or even in the country at large, don’t seem to understand what’s involved there. These are not uneducated people who live for conflict. Most want to avoid conflict.

So when government agencies ask me to serve on advisory boards, and particularly some of the military services have asked me to serve, whether it’s the Air Force University or the Naval Academy or similar, so long as they can cover my expenses, I do it as a way of giving back.

It also gives me an opportunity to ensure that they have the tools, and a constant reminder of some of the issues of character in the area of cyber. I don’t know how much of that I’m actually able to influence, but some of these awards in part recognize that I have had that participation and had that influence.

Do the government folks always get it right? No, that’s not the case. But looking at the world arena, I would rather have them trying and getting it wrong than some others being in the position to dominate the issues.

That isn’t meant to sound jingoistic. It’s not a my-country-right-or-wrong, you know, pr a it’s right or leave it kind of attitude. It’s a matter of it’s an institution that’s in place that has a lot of weight and authority behind it and insofar as if I can influence it, then I want to.

Several of my colleagues have refused, over the years, to get a security clearance, for instance, because they think they’ll be corrupted in some way if they go in and talk. I’ve had one for quite a while and what I find when I go in is if the conversation gets close to something that I think I might be doing, then I tell them. They excuse me from the room or change the subject. Whereas the things that are talked about where I can have some influence, they’re often glad to hear it.

The last couple years, that’s been less the case because I have been advising against some of the extremes that have been taken, I would like to see a better balance between offense and defense, and some of the people involved in making those decisions don’t want to hear that because it’s criticism. Not much I can do about that. But that’s been a layer that’s run through a lot of what I’ve done, and many of my students have gone on to do that as well. Better to try to advise inside than stay outside and pout.

Related to that is, I think, is an issue that Purdue is a very international university. There were some figures that recently came out where, I think that as far as public universities go, we’re number one or number two in terms of international population. We have *a lot* of international students. I’ve mentioned as we’ve gone along, students from Ireland, Austria, Mexico, Bolivia, Germany, I may not have mentioned their origin but I mentioned them by name. The majority of my grad students probably were not born in the United States. The majority of them now are U.S. citizens but at the time, they weren't. To me, the problem of information security is not how to dominate other countries. The problem to me is how do we make the infrastructure trustworthy enough that we aren't at the mercy of criminals and terrorists, and we can use our systems to be able to learn and to negotiate and talk with others. To me, it's much more important to defend all the computer systems that we have in the world, than it is to be sure that the computers that are in use by a current adversary are weak enough that we can exploit them. I think that strategy is, in the long run, a losing strategy.

I think the strategy of helping others to make their systems strong against random elements puts them on a better footing for us to negotiate with them, to deal with them as needed. It goes to that idea of trust across, really, the whole world.

And so I've worked very hard here, — we don't teach how to break into systems; we don't break systems. We are up front about things in the news. It's clear that China is conducting a lot of espionage. I mention that in front of Chinese students and they acknowledge it. But I also make clear that as a group, we're trying to work for more trustworthy systems worldwide infrastructure and that continues to attract very good people from all around the world. I hope it continues to do so.

It troubles me that we have people who view anyone outside the borders as potential adversaries or worse because that makes them that way; it doesn't create the opportunities. Even within our borders. I'm not a fan of people who break into systems because they can. I'm not a fan of people who harass others online, particularly those who don't have the skills to be able to protect themselves. And when that's done, I honestly think that's cowardly, that's wrong. But the fact that we have people who simply want to explore and push boundaries, it's more a problem that we haven't given them the opportunities rather than they're inherently bad.

I've tried really hard over the years to draw the line about ethical behavior, about what is good and what is not, about not teaching offense, about these kinds of issues, about not breaking into systems to demonstrate to somebody that they're wrong. But I've also tried to not demonize people who are experimenting and exploring. I think it's much more important that we provide good examples for them, and we provide guidance to help them. They're creative, they're imaginative, but once they cross the line too far, however, it's really difficult to bring them back because they either get a taste for it or the reputation. And if they haven't been able to distinguish where that line is, that's a problem, too. We have too much of that.

I, to date at least, haven't been harassed too much by that community. I don't go out of my way to seek it. I'm not encouraging it. I'm told that many in that community look up to me; some are scared of me. I don't know, I don't think there's a reason to be scared of me. But I go to some cons, and always have, and people come up to me and they've got 15 piercings, blue hair, and a Mohawk, and wearing an Anonymous t-shirt, I don't care any more than if they have on a business suit. What's on the outside doesn't matter as much as what's on the inside. So I think that kind of treatment of people is a thing that has helped in my career, as well. I don't judge based on on how people look. I've tried to make that especially clear, as well, with women and minorities. It's the mind, it's not what the mind's in, it's what the mind is and chooses.

Yost: Do you think that the computer security research community has been open to women?

Spafford: No, not as much as it should.

Yost: More or less so than computer science, as a whole?

Spafford: I can’t give you that kind of comparison easily. I think the nature of the difficulty is different. In computer science as a whole, we have a lot of people who view this as oh, this is mathematics and engineering, and it’s something men are better at. I’m sad to say that there are people I know who are very much like that. They’re wrong, but they won’t even consider that may be the case.

In the security realm, you’ve got almost a more aggressive group of people who, it’s an in-your-face, I-can-do-this-and-you-can’t, let’s-see-what-I-can-get-away-with type of attitude, and in my experience, that is not the norm for young women; if anything, they are more likely to be victimized by it. Many of them are put off by that kind of thinking and because it’s part of one aspect of the security mindset, you have a lot of people that when they sense that somebody’s recoiling or they’re avoiding something, they’ll zero in on that and really push. So if you have women in the field who pull back a little bit about this attitude or about some other behavior, some of these aggressive males will just zero in and pound on that. And that can be really problematic.

At least in the U.S. cultural background, there is some difference between the majority of women and the majority of men in the way they approach various problems. There’s no categorization that can say everybody fits in, but in general, the approach taken to various problems and the social interactions are different, and it's in conflict there. We need to do better about that. All the women I've met who are successful in this field are incredibly good. Now maybe that's because only the incredibly good ones can survive in the field, but they're really valuable colleagues and individuals to work in the area and we need more like that. So, yes, that's an issue.

Yost: And another topic on you wrote on your white board is "sense of humor?"

Spafford: I, as I said, I had to develop a sense of humor early on. I exercise it regularly. I don't see a lot of other people in academia at my level, and particularly in computing, who have anywhere close to the sense of humor I do at least in a public setting, but I think it adds to some of my security thinking. Humor, by its nature often involves unexpected associations and discontinuities. It's the unexpected: Ah, I didn't expect that! And some of it's very dark. A recent one that I heard that I told several people about this comedian by the name of Anthony Jeselnik, who has this line, "I spent the last four years looking for my wife's killer …but nobody wants the job." Well, there's an example of a discontinuity, a sudden shift that, if it were even a little serious it would be horrifying. But the fact that you were led one direction and suddenly snapped back is darkly funny otherwise. The fact is horrible from one point a view is part of why it is funny in another. Looking at the world humorously actually contributes to a security sense. You're not confined by the box where the system is. You actually have other kinds of perceptions, of the way things could be, and if you look at it with that sense of humor — and I try to cultivate a certain amount of that for myself and others around me — it can sometimes lead to a different point of view.

I think it’s unfortunate that to some extent, universities in particular and many work environments have tried to crush out humor, particularly any of the kinds that may be viewed as a little extreme. To me, to really develop this sense, every time you set up a boundary you constrain their thinking so that they’re not able to think about a possible solution or a discontinuity or a limitation.

That isn’t to say that I go around making a lot of sexist or racist jokes, or advocate crude humor that hurts or denigrates others, but there’s a correlation in that, I believe, if there are places we are afraid to go, that’s where you can set up the exploits, that’s where you can set up the bugs, because people won’t go there. I’m not proposing that humor being used as a security mechanism, but I think that there’s a connection in thinking that I’m sorry I’m not able to articulate better.

And it’s perhaps related here in that one of my closest colleagues and friends here on the faculty is Victor Raskin, who’s an international expert on humor studies, the ontology of humor. Not that he tells me jokes all the time, but he also has a somewhat unusual view of the world that seems to fit well in this regard. So I think it would be interesting if you were to look across all of the people you interview, there seems to be some characteristics, at least when I get together with some of these folks, they don’t particularly care what people think about them, at least they don’t seem to express it. They very often have a quirky sense of humor, Oh, and a lot of us seem to be current or former pyros.

Yost: That came up in the Becky Bace interview.

Spafford: Did it? She's got a quirky sense of humor that's just delightful, as well.

I guess last of all I'll mention some of the people that have been real mentors to me, I think it's worth mentioning. Of course, obviously, as I said, my sister, my parents, and my uncle all had significant influence on me early on; my sister still means a lot to me. She's got a PhD too, and is so smart. I don't think I was a very good brother, but I'm still trying to learn. My wife and daughter, certainly.

Dennis Martin, Sandy Miller, Jill Miller when I was an undergrad; as a grad student Jimmy Gough, Phil Enslow and Rich DeMillo on the faculty at Georgia Tech; but since then, Mike Atallah, Sam Wagstaff, Victor Raskin, all faculty here, spent a lot of time as mentors, as collaborators, as friends, have helped shaped what I do.

Outside Purdue, Matt Bishop has been somewhat of an inspiration from time to time. Steve Bellovin has given me critical advice, wonderful advice on occasion that's been very valuable. Corey Schou, on occasion, has given me some great advice. Becky Bace has been a constant source of encouragement and occasionally, inspiration. And Harold Highland certainly encouraged me in the early days. A gentleman who has just been inducted into the Hall of Fame, Jim Anderson is someone who had a big influence on me and others. And Peter Neumann has been inspiring and encouraging. My friend Simson Garfinkel has provided me with decades of interesting ideas and criticism when I needed it.

So these are all people that at one time or another have — or on an ongoing basis — have been very encouraging and very supporting, generous with their time and their advice. I don’t think anybody succeeds without that kind of assistance and I would really be remiss not to mention them. I fear I may be leaving somebody out in that list but those are people I can think of right off the top who’ve made a huge difference going forward.

I hope that 20 years from now as you or someone else interviews some others in this regard, that I might be mentioned in one or two of those lists, and that’s how we progress. It’s not solely through papers. It’s not solely through software artifacts. It’s really in the connection to help others achieve greater.

And if I’ve got to end anywhere, that’s probably a good place unless you’ve got some other questions.

Yost: No. Thank you so much. This has been extremely helpful to our project.

Spafford: Okay. I hope someday it makes amusing reading for someone. Thanks for your patience.