An Interview with

DONN B. PARKER

OH 347

Conducted by Jeffrey R. Yost

On

14 May 2003

Los Altos, California

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

Donn B. Parker Interview

14 May 2003

Oral History 347

Abstract

Donn Parker, a renowned expert on computer security, begins by discusses his education and early programming and managerial work at General Dynamics and the Control Data Corporation (CDC). The bulk of the interview concentrates on developments and contexts to Parker's subsequent work at SRI on computer security and computer crime. This pioneering research, which was funded by the National Science Foundation and the Department of Justice, provided Parker with the substance for a number of influential books. Parker also discusses the emergence of the computer security industry, IBM's contributions to the field, and computer security legislation. He concludes by addressing aspects of the contemporary computer security situation, best practices to prevent breaches, and his formation of the International Information Integrity Institute (I4).

This oral history is conducted for the NSF-sponsored CBI Software History Project.

TAPE 1 (Side A)

Yost: My name is Jeffrey Yost, and I am from the Charles Babbage Institute. I'm here today with Donn Parker at his home in Los Altos, California. It's May 14th 2003.

Yost: Donn, could you begin by telling me where you were born and where you grew up?

Parker: Yes, I was born in San Jose, California, just ten miles south of here. I grew up in the San Jose area. As a child we lived in Salt Lake City for a year, Chicago for a year, and Indiana for a year. I've lived most of my life right here in the San Francisco Bay area, except for 8 years in San Diego in the 1960's.

Yost: As your educational interests developed, did you notice a particular affinity you had for mathematics, or did you have a strong interest in mathematics?

Parker: I started out in engineering. And I got to my first engineering lab course and discovered that I had to get my hands dirty and do things mechanically with my hands. I decided that that wasn't my future. A neighbor was a professor of mathematics at San Jose State University and got me interested, so I switched after my second year to mathematics. Then I went up to UC Berkeley where I got my Bachelor's in 1952, and my Master's Degree in 1954. I didn't know where I was really headed in mathematics. At that time all you could really do is go into teaching or into industrial work in the oil

industry, to become a geologist type of mathematician. I didn't want to do either of those two things but fortunately, in 1952, computers came along. Of course this was long before computer science was established. So I oriented my interest toward applied mathematics, and started working on the earliest computers at UC Berkley, with the intent of getting my Master's Degree and then considering a Ph.D. I, however, began to realize that things were happening in the world in the development of commercial computers and I wanted to get my hands on that technology. So I decided to cut short my education after my Master's in mathematics and went down to San Diego to work for Convair Division of General Dynamics, where I got to be one of the first programmers on the UNIVAC ERA 1103 Computer. I got immediately involved in application programming, mostly in vibration analysis of F102 fighter aircraft, 880 and 990 Convair airliners, and the Atlas Intercontinental Missile.

Yost: So you were hired as a programmer?

Parker: That's right.

Yost: How many programmers were working there?

Parker: Well, there were maybe five or six of us to begin with. Then they brought in Dr. Charles Swift from the National Bureau of Standards (NBS), now known as the National Institute of Standards and Technology (NIST), who wrote the first assembler for doing symbolic coding.

Yost: That's the type of work you did the entire time at General Dynamics?

Parker: Yes. I was there from 1954 to 1962 doing that kind of work. And I went from doing vibration analysis, technically speaking, solving eigenvalue and eigenvector problems for very large, sparce matrices at the time, sixty by sixty matrices, to get the nodes of vibration of aircraft. So it was a matter of learning both computer technology and learning the application. I went from that application work to simulating an analog computer on a digital computer. And then I went into the management of the computer center for General Dynamics Astronautics, which is another division of the company.

Through my membership in ACM, which I joined in 1955, I got more interested in computers as an end in themselves. I decided that I wanted to work for a company where my area of interest was associated more directly with the actual product of the company, and I had trouble identifying with ATLAS intercontinental missiles. So I went to Control Data Corporation, where some of my friends from Convair had gone, up here in Palo Alto in the Stanford industrial park. So I came to Control Data in 1962 to work directly with computers as an end product. I became manager of the data processing service organization and ran a CDC 1604 and then a CDC 3600 computer center, doing commercial business for companies in the San Francisco Bay area. Then, not having great interest in running a business, I went back into engineering research. I worked on the development of the Control Data Digigraphic System, that was actually being developed in Lexington, Massachusetts at a division there that digitized and automated

engineering drawing using large displays. I worked on that for two years, and then Control Data said that I needed to move to headquarters to continue advancing my career. I decided life was too short to move to Minneapolis and so I looked around the San Francisco Bay area for another position. And I found one in 1969 through various associates to become the CIO, Chief Information Officer, at SRI International (Stanford Research Institute) in Menlo Park.

I served as the head of information processing services, and provided computer services for all of SRI. I did that for a couple of years and again decided that I really didn't like the management career route, and that I was more technical and research oriented. At SRI a group of criminalists had a grant from the National Science Foundation to study various aspects of crime. I used to eat lunch in the cafeteria with these people and told them that I had a file of computer crime cases. They said, "What kind of crime is that?" So I described what I had collected and my interest in that area, and they said, "Why don't you write a little report on that for us, for the NSF?" So I wrote a report and they submitted it to their monitor at NSF who said, "Hey, NSF's purpose is to fund new areas of research and no one has ever done anything on a subject like that before. Why don't you do a planning grant project?" In 1971 I planned how I would study and report on this new emerging problem of computer crime. They thought this was a good idea, so I submitted a proposal and got a second grant to do that research, and this led to eight years of grants that were relatively small and did not pay for my full-time participation. So for those eight years I, and an associate, Susan Nycum at Stanford, did this work until I became an embarrassment to NSF because they do not fund researchers on a continuing

basis on the same subject time after time. So the director of the NSF called me in and said, "We have to do something. We want to help support you in continuing this research but we can't do it within NSF. We will find another government agency that can fund you on this." So they referred me over to the Department of Justice's Bureau of Justice Statistics. I submitted a proposal for a grant to continue that kind of research, and they gave me another grant , and for another six or seven years they funded me, again, not at very high level but in a series of small grants over that period of time.

Yost: What first got you interested in computer crime?

Parker: Yes, I need to back up here to that part of it. In the 1960's I was very active in the IBM Share Organization. So I had a great interest in professional associations, and ACM in particular. I was chairman of the chapter of ACM here in 1963 when I first came back to this area, and then I was elected to be a member of the ACM National Council. I was on the ACM Council for about ten years, and then I was elected National Secretary of ACM. While I was on the Council, a position was opened on professional ethics, Chairman of Professional Standards and Practices Committee. My interests had always been in finding interesting things to do that others had never done before. In a way it made the work I did more exciting and easier to do because I had no competition. I had no competition, no one was particularly interested in professional ethics in ACM at the time because most of the people in ACM, especially the leading people, were computer science academics, as they still are to a great extent today. They were not interested in professional ethics. I was one of the few people in the council who came

from industry. So I did some study, particularly looking at other engineering areas, and the professional codes of ethics of the chemical engineers and industrial engineers, mechanical engineers, and so on, and decided that we needed a code of ethics in the computer field and that DPMA had not done much on that. The IEEE had a code of ethics but it applied to them as an engineering society rather than their fledgling computer society. So there just wasn't anything on ethics in the computer field, and I noted that computers were increasingly important in business, research, and government.

Ethics issues started to arise, having to do early on with the idea of who owns a computer program.

Yost: What was the opinion of the academicians in the ACM?

The academic people in ACM said, "Oh, computer programs are not owned, they're just in the public domain. Everybody shares software." Well, it turned out that the business world discovered that they were investing huge amounts of money into software, and that it was really a commodity, intellectual property, that required buying and selling. This got the academic community very upset with the idea that you buy and sell computer programs. Well, that took hold, and along with it, of course, the issues of people doing bad things: stealing trade secrets, selling and using computer programs they didn't own. So those kinds of things started developing and requiring ethical principles on which to base this industry, beyond just the hardware engineering side of it. We needed ethics to govern the software side. As a dedicated Christian, I also had a great deal of interest of

ethics from a religious perspective. So, I thought, "this is a great way to combine my application of my Christian values in a technology." So the whole thing came together. I started developing, along with a committee of people that I got together, a draft code of ethics. And very quickly it turned out that a code requires enforcement, and academically ACM wasn't an association that was going to enforce something like that; and secondly, it's really not just ethics, it's broader, it has to do more generally with acceptable rules of conduct. And so the Council limited me down to developing a set of guidelines of conduct. And under that rubric I said, "O.K. I can do that too." The Guideline of Conduct was adopted by the ACM, and has since gradually evolved.

Along the way I got two National Science Foundation Grants from the EVIST, the Ethical Values in Science and Technology Division of NSF, to do some organized research on ethics in the computer field. In 1976 and ten years later in 1986, I did projects on ethics where I created over a hundred ethical dilemmas in scenarios, and I then gathered together top leaders in the computer field, from the industrial business side, the academic side, and from government. I got several industrial psychologists and a couple of ethicists involved as well. I had about twenty people. And I got them together for two days at SRI, after they had studied these ethical scenarios, and we debated these ethical dilemmas associated with computers; who owns a computer program, using others' computers, and that type of thing. And then we voted, I had these people vote whether the actors in these scenarios were unethical or not unethical - I didn't asked them if they were ethical, just whether or not they were unethical. We compiled and gave them the results, and I'd give them more scenarios and narrow the key

issues. I wrote two books on ethical conflicts in computer science, engineering, and business, following each of those projects.

Yost: With the ethical dilemmas that you presented, were the people from industry and academia on opposite sides on the issue of the proprietary nature of software?

Parker: We did these projects twice, ten years apart, to see what kind of changes might have evolved. And there were some changes, the primary one probably having to do with the concept of owning computer programs; the academics tended to be more liberal in that regard, and the industrial business people more conservative in putting more stock into the value and profitability of software issues. There was also some evolution as well that had to do with the way computers were used; a computer in a room, in a building, in a city, and you shipped you're stuff in on paper and they ran it for you in the computer and delivered the results back to you physically. So you had to go to the computer center itself to take your jobs there and get your results back, and so on. So there wasn't the personal freedom or involvement with the computer, it was walled in by people who ran the computer, and they are the only ones that had access to the computer. Then ten years later, 1986, we had gotten to the emergence of PC's and workstations. So there were some dramatic changes, and the ethical values didn't change for these people, but how they were applied, and what they pertained to – like I was saying, in the early days you could give computer programs that your company spent several hundred thousand dollars developing, and just give it to somebody at a competing company. And nothing was said about it. Ten years later, you'd go to prison for doing that. The programmers and

systems analysts and the academic people all had a difficult time in the transition from one concept to the entirely opposite concept, and this led to a lot of ethical issues: Who owns the cycles in a computer? The computer's sitting there, if no one's using it, I want to use it, and I should be able to use it and not have to pay for it or anything like that. Well then the service bureau started charging time, computer time costs money, they discovered. And so that all developed.

I was running this commercial computer service center for Control Data in Palo Alto in 1964-65 and one of our programmers was doing work for our clients, working as my employee. He was a graduate student at Stanford, and I caught him selling his services to his own private clients, in competition with me essentially, and using our computer free of charge to do this. He would come in at night, when no one was around and use the computers, "Well it's sitting there, no one's using it, why can't I use it?" So I had to fire this programmer and he was a rather odd, difficult guy. In fact, he terrorized me and my family for a number of years following that incident with telephone calls at 2:00am with heavy breathing kind of stuff. When I had to fire this guy and I was involved with this ethics work, I started noticing newspapers articles here and there about programmers going to prison, and being arrested for crimes associated with their computer work. So I started collecting these news articles in part to defend my position of having fired this guy. And coupled with my interest in the guidelines of conduct I had done for ACM, I was trying at the same time to promote the idea of the code of conduct for ACM, but there continued to be resistance. And I said, "Look, people are being arrested, ACM members are being arrested for violating their trust in their profession." It is a direct

concern to ACM. So I had a collection, from 1962 to 1969, of several hundred news clipping versions of these cases. So I had that when I went to SRI, I didn't have an idea yet of having this as a career, or anything, or doing work on this problem. But in 1967 Dr. Willis Ware, who I considered to be the senior statesman of the information security field at RAND Corporation, ran the first panel session at an AFIPS Spring Joint Computer Conference in Los Angeles, on this subject of computer security; no one had ever done that before. The only work that had been done was mostly cryptography and secret work being done at NSA, and primarily concerned with military traitors. And so all of a sudden there was some interest from the business, industrial, and academic world in this subject of how do you protect this information; how do you protect these computer programs.

Yost: Was RAND initially looking at national security issues and then it evolved into other areas?

Parker: I don't know very much about that because that was all a military secret. So Willis can answer that better than I can. All I knew was Willis wears a public face and he presented himself to the world – RAND was pretty much limited to doing work for the Air Force. So I knew only of Willis Ware's work primarily, and Paul Baran at the same time had some interest in it, he wrote some articles on that which became public.

Yost: You mean he wrote a couple RAND Reports?

Parker: Yes.

Yost: Both Paul and Willis, and especially Willis became heavily involved in information privacy. Can you speak a little bit about the relationship, as you see it, between privacy and security?

Parker: Alan Weston and Robert Ellis Smith were some of the earliest people who were concerned about privacy issues. I looked on privacy as just one piece of the whole threat issue. I had a concern for privacy as it related to: "How do you protect personal information in computer media any differently than you would with paper media?" Privacy developed primarily in the federal government, and state governments. But I didn't see it particularly, in the early days at least, in the business industrial world at all. Alan Weston and Robert Ellis Smith gradually generated interest and it did, obviously, develop and become an issue in the business world.

Yost: I know Weston was a legal scholar, was Smith as well?

Parker. No, he was a journalist. He published the leading newsletter on privacy[*Privacy Journal]*. He exploited the privacy issue with his newsletter and he was thought of as kind of an extreme reactionary, crying in the wilderness, "Hey, there's a privacy problem in the business world." The business world in the 1960's and 1970's did not like the need for information security and privacy; it did not contribute to profitability, productivity and growth- in fact it subtracted from those things. The concept of business

crime was considered an embarrassment that nice people in business did not discuss. The people who studied embezzlement – I worked with one of those, Donald Cressey, who was a famous criminal sociologist who worked with a man named Sutherland who invented the term "White collar crime." The business world did not like what they were doing, and it turns out they didn't like what I was doing either. I had to be extremely careful in what I said and wrote concerning this problem. And that's where I had to severely limit myself in naming the victim companies of computer crime because the next thing I know, it would be in the newspaper. I was interviewed by Dan Rather and Gerarldo Rivera, and Tom Brokaw, 60 minutes, 20/20, all the morning shows, and the evening magazine shows; they all interviewed me. The news media just grabbed the subject of computer crime and ran with it. They thought it was the greatest thing since sliced bread.

Yost: This is the late 1960's?

Parker: Yes, well, I'd say the mid-seventies was when it all hit the fan. And the business world, as I say, didn't like this privacy stuff. The banks had a great motive to protect the privacy of their customers, but in their own way, and for their own benefit. So Robert Ellis Smith was an outcast because he was saying, "Banks, look at what they're doing with you're private information, they're selling it!" So the business world tried to stifle this concern and growing interest in privacy, as well as computer security generally regarding how to deal with the protection of people's personal information. People often confuse things and say, "the privacy of information", which is wrong. Privacy is a

constitutional right, they mean confidentiality of personal information, not privacy. Anyway, I was struggling because I was a part of the business consulting organization at SRI, and our business came from working directly for very large international companies. Here I was running around talking about bad things happening in business, and business didn't like that at all. I came close to getting fired from SRI once when a newspaper reporter associated my name with the name of a company that had been a victim of computer crime. The president of SRI had to defend me from this member of the board of directors of SRI. Something that has never been recognized, explicitly, in the computer security and information security field, is that everybody hates security. I can't stand security, I hate all the password stuff and having to diddle with anti-virus software and paying money to protect myself from crime; I hate all these constraints on me, everybody does. Everybody likes to be able to communicate in confidence and secrecy when they need to and everybody likes to have an assurance that they are free from attacks from criminals, but as far as security itself is concerned, I mean the locked doors and filing cabinets and then ultimately having to lock your computer, is unpleasant and inconvenient and it subtracts in business from profitability, productivity, and growth. So nobody likes it. So I've spent thirty-five years of my career working in a field that nobody really likes, it's been kind of interesting. The journalists like it for the sensationalism; it sells newspapers; you can get people disturbed. But otherwise…

Yost: Can you speak a little bit about your relationship with the journalists. In one sense they are providing some of the data and information that you're following up on and using in research, and then they're also looking to you for guidance on the issue.

Parker: I wrote the first definitive book on computer crime, published in 1976.

Yost: That was *Crime by Computer*?

Parker: Yes. However, another book had been written three years prior to mine by Gerald McKnight who was a journalist in London. He wrote a book called *Computer Crime* and he used all of my cases and input in actually writing this book. It was more of a general trade book, whereas mine was the first book that addressed it from the point of view of a technologist knowing computer technology, and describing computer crimes in those terms, on a more scientific basis and based on the computer crime research I had been doing that was funded by the National Science Foundation. But journalists hopped on this right away, very early, and anything new that would scare people and say the world is falling apart, something entirely new, using giant brains to carry out horrible huge crimes. So there was a tremendous interest and I certainly benefited in a way from that attention because the NSF was just deliriously happy with the work I was doing because it was getting this huge attention in the news media and I was the only person in the world who actually, knew anything about this problem, because a great amount of what I and my associate Susan Nycum did with these NSF grants, was to go out and track down the criminals involved, and the prosecutors and the victims.

TAPE 1 (Side B)

Parker: I was collecting lots of the documentation of these cases we were finding, and Susan and I were out collecting our own first-hand information, primarily from computer criminals who were very cooperative, for about ten percent of the cases. So we had all these wild tales that we could talk about when the news media came to us. We were the only source that they had, actually . I was getting about a dozen calls per week from journalists during the 1970's and 1980's.

Yost: Were these computer criminals willing to talk with you when you approached them?

Parker: Yes, they all were all eager to talk. And we used several techniques to get them to open up. There were different reactions depending on whether you were going after these people to interview them before their indictment, after their indictment, during their trials, after their sentencing, and during the time they were in prison, and then after they were out of prison. We were able to interview several of these people in different stages. The public generally thinks bad guys are career criminals with an evil glint in their eye and ready to do anything to engage in crime. And that's not what crime is all about to a great extent. I think mostly it has to do with ordinary people, lots of them in positions of trust who are attempting to solve personal, unshareable, intense problems. We interviewed these people in prison and they said, "What am I doing here? I'm not a criminal? I had this terrible personal problem I was trying to solve. And I found that violating my trust and doing what I had to do caused the least amount of harm to the least number of people and got my problem solved. I'm a problem solver, not a criminal."

The news media made it sound like computer criminals were motivated by greed and high-living. Well this guy stole ten million dollars out of this funds transfer system, obviously greed and high-living was his motive. Not true. And we did come across several what you'd call career criminals who earned their living or part of their living by criminal activity. But not very many, especially in computer crime, high-tech kind of crime. These were all people you could interview and say, "There but for the grace of God, go I." They were people who had got themselves into a personal jam of some kind: a manger in a business whose department was doing badly and was going to be fired if he didn't do something and so he changed the data in the computer that made his department look better this quarter and he'd make it up next quarter. Well that's a crime, and he'd get caught and convicted of a crime and he's sitting in a prison cell, "What did I do? I was just trying to help my company. I was trying to help my employees so I wouldn't have to lay them off." So it's every personal problem you could possibly imagine: Sex, competition with your bother-in law, a gay person whose partner was threatening he would leave him… These are the motives behind computer crime.

Then, of course, we got into the hackers phenomenon that started with phone freaking back in the 1960's; Captain Crunch, hero of the phone freaks, and Steve Wozniak and Steve Jobs of Apple fame, who were selling illegal blue boxes to defraud telephone systems up in Berkeley – all those stories that started with an article *in Esquire* Magazine – I had forgotten the exact year but it was around 1971. A very famous article that for the first time described hacking. It didn't call it hacking, it was phone freaking and then about the students at MIT who were controlling their model trains with computers and

started seeing weaknesses and compromising, and playing practical jokes on one another with personal work stations and so on, that started the whole hacker kind of thing. So we ended up with an entirely new kind of criminal; not so new if you say juvenile delinquents playing practical jokes that got out of hand, and then given powerful instruments to continue their practical jokes. Otherwise you'd have to say it's a new kind of criminal that we have to face. So a great amount of what we dealt with was not just the white-collar problem solver criminals violating their trust, but people outside of the position of trust attacking inside businesses. For the first time in history, business found juveniles running around inside their accounting and engineering systems, and they'd never had that problem before, and here they were on their electronic doorstep. Of course that created a whole new wave of media attention. So we got into the movies; I worked with the writers of "War Games" and "Sneakers" - they were going to do a trilogy, but they haven't done the third one yet. This is Walter Parkes and his associates, the producers of those movies. And so the press, the news media, movies, and the T.V. were saturated with this stuff during the 70's and into the 80's. You'd think they'd get tired of it, but even today there's still a tremendous amount of interest. Even the most innocuous cases, if the reporter can associate it with a computer he's got a front-page story not a page twelve story. So it was natural for that kind of thing to proliferate.

While I was doing the computer crime research I was working on developing the security side of it; how to stop computer criminals. I was lecturing and writing; I wrote six books; I did reports for NSF and Department of Justice; I was giving sixty to a hundred lectures per year on all this stuff. The interest and concern was world-wide: the Swedish Press,

and the Russian Press, Chinese and Iranian Press. So it became of world-wide interest. As each new advance in the technology proceeded, crime obviously found a way to proceed right along with it. So with every new technical advance, there was escalation and advance on the crime side.

Yost: Did you notice significant differences internationally, or did you ever study computer crime in different countries and different cultures?

Parker: Yes, to some extent. I think we explicitly reported on that, just a paragraph here and there, in some of the reports we did. The United States, being the most advanced by far in computing, was the most advanced by far in computer crime. People in other countries looked with awe on the advancement of computers in the United States, and they happened to also look on it by seeing all the news media on crime. Well, "Only in the United States", you know, "Huge crime source, that would never happen in our small little country." But they were anticipating, as they had with the spread of other technologies from the U.S. to the rest of the world, that computer crime was going to spread as well. So there was intense interest around the world on computer crime in this country. And then it started to careen in other countries; in the U.K., for example, I started discovering a number of cases but they were kept highly secret. It was easier in those countries, even in the U.K. to restrict this kind of information, especially in large businesses. A lot of those large businesses, large banks in the U.K. and Europe were my clients on security. And so on the inside I knew what was happening to them. There were some spectacular crimes starting to happen over there, but you didn't hear about it;

the news media didn't get a hold of a lot of it, because they were able in those more private or restrictive kind of countries to hide this kind of thing. Sweden, Finland, and the Soviet Union, in particular, we had just heard little bits and pieces of things that might be happening in that part of the world. In Japan, a very different culture, especially from a crime perspective, they had organized crime, but suppressed any kind of information about unethical activity: abuse, misuse of business assets; and abuse and misuse of computers. As they became much more advanced in computers, I did a lot of security work for large companies in Japan. They prided themselves on the idea that business crime doesn't happen in Japan. I worked with the Japanese police for several years, in fact I trained some of the Japanese police in doing computer crime investigation as well as Interpol, Scotland Yard, the Royal Canadian Mounted Police (RCMP), and the South African police. The Japanese anticipated that this was going to be a problem, but it wasn't visible for a long time. Japanese computer crime lagged the U.S. by ten or fifteen years.

Yost: Without mentioning any clients, was there any sense you got from some clients, or potential clients that they did not like you to publicize the issue as much as you did in your writings?

Parker: Very much so. That was an extremely difficult balancing act because on one side I was doing computer crime research, discovering bad things happening in business, and at the same time I was a consultant to them, helping them to develop protection from these kinds of problems. I was able to associate myself with the auditors and the

industrial security people in these large companies as long as it was kept confidential and limited to working with those kinds of people. On the other side, the publicity of this problem, and my exposure in the news media was a problem for me, and I had to control that in some way. It developed into a love-hate kind of relationship and my clients required my not saying anything about them at all in the news media, and I worked hard to try to present myself to the journalists as a computer security specialist rather than as a computer crime investigator. When they wrote their articles I'd be happier when they quoted me making some kind of general statements about the problem and then later in the article are details about the crimes that were going on. The closer my name got to the part of the article where they were talking about crimes, the more nervous I became, and more concerned that I became. And I did make significant efforts to try to represent a business perspective to this whole issue; yes, there are business crimes involving computers, but crime has always been a problem and the business community has rallied to deal with the problem and has extensive auditor functions and industrial security people to deal with it. So I got by, and I was able to balance both kinds of activity. The business world appreciated that I was studying computer crime that made what I had to say more valuable to them. I and very few others have ever approached information security from a crime perspective, from the criminal perspective, and that has given me a unique and quite different view of information security than most of the people in information security today who have never met the enemy. For instance, most people in information security think in terms of prevention, detection, and recovery; that's their world. I look at it much more broadly from the point of view of avoidance; removing suspicious people from positions of trust, for example; and deterrence, how to stop kids

from even thinking about getting involved in malicious hacking. Many people working in information security have not thought about avoidance or deterrence, and also sanctions or penalties against people and rewarding people for good security. So I keep crusading. I'm known as a "contrarian" in the information security field because I'm one of very few people who take this approach.

Yost: Why do you think they look at it in such a limited way?

Parker: Well, it's not a matter of complaining about them because information security is extremely complex from a technological perspective. Most of the people in information security today are putting out fires; they're trying to deal with the technological aspects of attacks and defense. And that is by itself a full-time occupation. And it's necessary that we have people, maybe the majority of people in information security who are dedicated computer technologists who can deal with extremely serious problems of vulnerabilities in computer systems. So no, I don't take away from them in that regard, it's just that we need the broader kinds of people in information security as well who understand that risk-reduction is not a viable objective in information security. Because risk is not under our control: we cannot manage risk, we can't measure it, because risk is produced by our unknown enemies and we don't know who they are, what they're thinking, we don't know their skills, knowledge, resources, access, authority, motives, and objectives; we don't know what they have against a particular company or a particular government organization or the 200 million people on the Internet world-wide today. What you are able to control is security and some of your vulnerabilities. Thus,

we need to do security management, vulnerability management, but not risk management. I am in strong disagreement with a number of people in the information security field on the subject.

Yost: So is it perhaps more a question of executives at companies realizing that in addition to information security technologist they need other people working on these issues with a broader background?

Parker: Yes, I think so. And I'm pleased to see the broadening of interest within the academic world, within the professional world, of people in other specialties who are focused on computer crime and the computer security problem. I'm finding social psychologists, I'm finding people in the law profession particularly – Susan Nycum, who is a lawyer who worked with me very early on the computer crime research. She was one of very few people in the law profession doing research in this area, and she did it only part time. She had her own law practice.

Yost: So she wasn't part of SRI, she just worked with you on that?

Parker: That's right. She was a sub-contractor to us on our grant. So she would deal with the legal perspectives and I'd deal with the more technical perspectives when we interviewed computer criminals. So we found a psychologist who developed an interest, and the U.S. government had a group of psychologists and psychiatrists studying the problem of traitors in the military, and they had very strongly turned their attention to the

computer crime problem. So it's been very satisfying to see more and more of these people. In the criminal justice community, I trained the first three or four detectives to become computer crime specialists. Then that grew and today every big police department in the world has a computer crime section now. In the 1970's there was no such thing. I helped form detective departments, but they went out of business very quickly because they got all trained and ready to go and said, "O.K. , where's all the computer crimes we investigate?" And nothing happened because computer crime was just thought of as another kind of crime. The Department of Justice's Institute of Justice and the U.S. attorney's view was that there was nothing special about computer crime, "These are embezzlements, these are industrial espionage, these are murders, rapes, these are pornography crimes, they're not computer crimes." Then we started to realize that the criminal law was inadequate in some cases. And so I started working with Bill Nelson, state legislator in Florida, (now a U.S. Senator) and helped him get the first state computer crime law established. Susan and I both helped him do that.

Yost: When was that?

Parker: That was in1978. Then a couple of years after that California adopted it's computer crime law, and I worked with the people on that. Then the Federal Computer Fraud and Abuse Act in Congress was developed. I always claimed that the need for these statutes was not because we couldn't convict computer criminals. Instead, these laws were more of a social statement that told the world of the importance of getting back to ethics, that doing these kinds of things, using someone else's computer, violated their

privacy and in fact was a theft of services and should be treated as a crime. Having specific computer crime statutes was a way to establish a social agreement that these were real, serious crimes. The other purpose of getting specific statutes was to help law enforcement agencies get the budgets they needed to develop the capability to ultimately be able to deal with investigation and prosecution of computer crime. Those are two purposes that often are not recognized as reasons why you need a criminal statute of a particular kind. There are still more arguments now about what is unique about computer crimes. And there are some statutes that tend to be so esoteric that many prosecutors are still using old criminal statutes rather than the new computer crime statutes to prosecute these cases; the penalties are greater that way, and juries can more easily understand traditional criminal statutes. So my advice in training criminal justice people is, Rule 1: try to eliminate the role of the computer in the crime so you can treat it within your own knowledge of traditional crimes; Embezzlement is embezzlement; and don't try to get the technology involved in the prosecution because juries don't understand the technology well enough to deal with it. And Rule 2 is: if you can't avoid getting the computer identified and involved in the investigation and prosecution of the crime, get an expert to assist. Because you as a detective are not going to be sufficiently expert in the particular computer system, the particular application, the particular code that may have been involved in a technological crime. Gradually there are increasing numbers of detectives and prosecutors and lawyers who are expert in the technology side as well as the law side so that is another area where I'm pleased to see the development of these specialists. Unfortunately, in the criminal justice world, the police and prosecutors are not allowed to specialize. Once you become a specialist in one area, the next thing you know you've

been moved to another area. So a detective has to be a detective who can deal with drugs, murder, and computer crime. This was frustrating for me for many years because I trained these detectives to understand computer crime and they had to spend a huge amount of time learning enough about it to be effective. The next thing I know the person says, "Oh, I'm not in computer crime anymore, I'm moved back over into drugs." So we've lost all that talent. And to this day police organizations advance and reward people depending on their generalist capabilities rather than their specialist capabilities. Some of the detectives who have stuck it out have suffered in their careers for doing that. So I've been trying to get law enforcement agencies to understand that this is a world of specialization and it has to include police as well. It's been fascinating work because on one hand I'm dealing with the law, and on the other hand I'm dealing with bits and bytes on computer. I am also dealing with social psychology and criminal psychology, and business systems. Susan and I, in the 1970's, had to try to become experts as much as we could -we were really amateurs- in this wide array of specialties to deal with this multi-faceted problem because no one else was – there weren't any other lawyers dealing with it. There weren't any other criminal psychologists who even knew what a computer was. Fortunately, that's gradually changed.

Yost: Could you speak a little bit about the security industry and how it moved from individuals and small consulting operations to major corporations?

Parker: Yes, the computer security industry started with one company, really, IBM. IBM was one of the earliest companies that publicly recognized the need for security and

recognized that there were bad guys who would use computers for bad things. They had some two-page advertising to that affect in the late 1970's. They probably had the first specific product, RACF, that was, or is- it's still a viable product today – an authorization package so that you had password-enabled usage and using RACF you could associate individual people with access authorization to individual files. Then another company, and I can't remember the name of the company that produced ACF2 and Top Secret, but ACF2 was a competitive product for RACF. These three products were the primary products that you could buy to deal with information security in computer systems. Then the issue of how do you authenticate the identity of people to know that this person who gave this password really owned that password. So the field of biometrics started. And to this day, the biometrics part of the computer security industry has come along very slowly and very much up-and-down because, again, people didn't recognize the point that I made earlier, that everyone hates security. The idea of having to do something to be authenticated was not an acceptable idea, thus, commercially the products failed. One of the problems of the computer security product industry was that they believed the news media. The news media was creating this huge problem happening to us now; that computer crime was destroying the world. And so hundreds of little companies started developing security products because they believed the headlines. The venture capitalists would read headlines about the horrible things happening to organizations through computers and they thought, "My gosh! There's a product there! There's industry there!" And so they would invest money and build a security product and, as I say, the business world, government world, hated security. They weren't going to spend much money on security. Our consulting work kind of dribbled along. We'd get a thirty

thousand dollar consulting contract and think that was really pretty big. And my associates over in inventory control and marketing were getting three million dollar contracts from some large company. It was ordinary, oh yeah, sure, three million dollars. Well we never came close to getting a million dollars worth of a consulting contract because there wasn't the accepted idea that a business would actually pay money to do something about computer security. So top management in business would listen to Dan Rather on "60 Minutes" and listen to me emoting and so on, and they'd just kind of get mad and go to their industrial security people and their auditors and say, "What's all this stuff I saw on T.V. last night? It doesn't look good for us to have all that computer crime exposed. What's computer crime all about?" Auditors and industrial security people didn't know anything about it. "It's all those geeks over there in the computer center, and we don't know what they do, but we don't have any problems like that." Business executives would say, "Where's the problem? We don't have anything like that." Many of them did have problems, but they were buried in the technology, they were buried in the company so that I'd come in and do a security review and find all kinds of abuse and misuse of their computers and their software and software pirating. But it didn't get up the line to where top management, where the CIO, let alone the CEO ever even were concerned about it. They didn't like it, and they didn't want to spend money for a problem they didn't think they really had. Security did not favorably affect the bottom line so why spend money on it? So we inched along during the 70's, 80's, and into the 90's because of the nature of the problem. So biometrics finally, I saw an article this week: "Biometrics industry finally coming into it's own" it is now established. I still have doubts. I used to consult for a lot of these little security product companies, and

they were producing all kinds of fascinating individual products. And of course when computer viruses came along, the anti-virus software immediately became a very big thing. But these little companies would come up with these little biometric hand print and eye-scan products and really wild ideas, and then cryptography became of interest and hundreds of little companies developed new crypto products. I consulted to a lot of these companies and they would call me in to look at what they were doing and I said, " Oh, I'm sorry you guys, but you're believing what you read in *TIME* magazine. You're believing what you read in the newspapers and see on T.V. I'm sorry, there is no market for your product. My clients, the people who would buy your product, they're not going to buy this stuff. In the first place, you're too small. They're not going to make a giant corporation dependent on two guys in their garage who developed this fantastic new security product." I said, " You'll never succeed, just two guys or ten people with a couple hundred thousand dollars. They're not going to trust you , you're going to be gone next week. Why should they put their entire corporation at risk based on you're product. You're not going to control the risk anyway." So I was maybe instrumental in helping these little companies go out of business more quickly than they would otherwise go out of business and avoid a lot of the pain. Finally, in the late 1990's , in the last five years or so, the industry finally has established and has come into it's own. The biometric part of it is still lingering along and "Smart card" technology fumbling along, doing some business and starting to get successful.

TAPE 2 (Side A)

The whole industry got deceived by the news media attention given to computer crime and security. And, in fact, the little companies got lots of exposure at first when they first blossomed with their new cryptographic products. And then they'd go out and try to sell it and they'd come to me and other people in the security field, consultants, and say, "Where's the pony? There's a pony in there someplace, Dan Rather said so!" And I'd have to explain to them, " I'm sorry, but everybody hates your product, from the point of view of not wanting to pay for it, not wanting the inconvenience." And so I tried to advise these product companies, "Make your product transparent so that it's unseen." But of course they're proud of their product. They put their logo on it and they want it to be seen. I said, "You don't understand the security field. It's got to be transparent; it's got to be unseen; and it has to have minimal affect on people's activities." They couldn't stand to have their product under the table or hidden someplace where no one would know that it's there. I said, "That's the success of your product. That it's there and working and nobody has to know that it's there and working."

Yost: What about IBM? It was a company that did get into this area and it came out with the two-page ad on computer crime in many publications.

Parker: These giant companies, IBM's customers, knew that they had to restrict access to the proprietary information and in particular to personal information: the payroll, social security numbers and bank accounts. It became pretty obvious that personal privacy mattered. Large companies accepted that you had to have a security product: and RACF

was the only thing available, and then ACF2, and a couple of other smaller competitors. But that was just about the only market that there was. The military - and that's a whole other world of information and computer security – the military obviously needed computer security and the NSA became the expert source for knowledge about military security. And then Abraham Ribicoff and Patrick Leahy and some of the other Senators forced NSA to assist the rest of the world, the business world, and the rest of the government in protecting themselves in the use of computers. NSA only knew confidentiality, only knew secrecy. And so in the early days, in the 60's and early 70's, confidentiality and security were synonymous in their world. You asked someone at NSA about security and they used the world security but they meant confidentiality. The "orange book" (the DOD's *Trusted Computer Security Evaluation Ctiteria*, first published in 1983) is a milestone. The DOD produced this manual that described several different levels of security that computers were to have, claimed that it dealt with all aspects of security but in fact, it didn't, it only dealt with secrecy within a computer system and not false data entry or deception kinds of issues. And intellectual property ownership was not an issue, they didn't worry about that at all. So here were Air Force captains trying to figure out what banks and insurance companies needed - it was a bad fit. They just didn't mesh and didn't understand at all. At the deepest technical level they did, but the characteristics of these controls and their affects on the people involved were entirely different because the objective of the military organization is security, and the objective of a business organization is profitability, productivity, and growth. And the objective of a government agency is service within budget and those are incompatible with the military objective of security. So people outside of the military in

their work environment knew that, although they were told that they had to apply information security to their work, they knew that it interfered with their job performance. So even today I'm crusading for the idea that for security to succeed it must be a part of job performance rather than being in competition with job performance, which it generally is until a company or organization says, "Hey, you're going to get a promotion, you're going to get a salary increase, based in part on the extent to which you cooperate and support the security of the information in the systems that you work with." Until that happens, and it hasn't happened yet, security is going to take second position; it's only cosmetic and superficial.

Security is not successful outside the military today because the motivation for security has never been addressed. Way back at the very beginning we realized and understood that those of us that were working in information security with a real "against the enemy" kind of security. Like I say, most of the people in security were working on it from the point of view of: here's a kind of attack, here's the technological change in vulnerability and technical controls to deal with that attack. And that's what information security – maybe 80 percent of it – consists of today, and it always has from the very beginning. So until it gets moved out of the IT world and into the industrial security world…and that's an interesting aspect about how computer security developed almost independently of industrial security. These two responsibilities, the information security officer, and the industrial security officer hardly even knew one another. Often in my consulting assignments I was the first one that brought them together for lunch, and I said, "Hey I want you two to meet one another. This guy deals with bad guys and this

guy deals with technological controls to protect this company's information from bad guys. You two ought to get to know one another." And to this day these two departments are in separate parts of the company, totally different areas; they're staffed by entirely different people, retired policemen over here, and computer technologists over there. And if either one of these people reverted to their base career, those people would go back to the police department and these people would go back to IT. This dichotomy has been there since the very beginning and from the very beginning we worked to try to bring them closer together, and we've been doing that for the last thirty-five years but with limited success. Several extremely large companies did make some significant progress in putting them together and, in fact, one large company I worked with put them together for about three months and then had to pull them apart again because it wouldn't work.

Yost: And was that decision made at the very top?

Parker: Yes. It was an airline, and the industrial security people were mostly ticket fraud detectives and here were these computer technologists and they put them in the same room together all inter-mixed and they were the total security function of the airline. These programmers sat there and looked at these ticket detectives across their desks and said, "What am I doing here?" It was headed by an ex-FBI agent who headed the fraud detection part of the company. These computer technologists said, "He doesn't know anything about computer technology. I'm not going to get a raise, he doesn't even know whether I'm doing a good job or not. I'm not going to stay here. I want to go back

to where I'm familiar in the computer center, in IT. That's what I am, I'm an IT person." So they had to pull them apart. The security industry developed, starting really with the anti-virus software, and that really was the thing that got it off the ground because prior to that, these two products, ACF2 and RACF, was all that anybody thought ever was needed. And then of course the PC came along and the Internet and the need for putting a device between a computer and the Internet world became an essential security device. And so firewalls were created. Previously, we had a few secure switches, secure modems, and then the firewall as a proto-security product with no other purpose except being a security product developed. Up until that time we were trying to help the security industry by saying, "people are not going to buy a security product, people are going to buy a modem that has security in it; people are going to buy a PC that has security in it or they are going to buy a computer that has RACF already in it. And they're not going to spend money for a discreet security product." And so my advice to them was, "You should be an OEM to the companies that produce all the various computer and communication products providing your security as an integrated part of their product." These people with pride of product and the idea that the news media said they needed these products, and we're going to provide them, they went out of business pretty quickly.

Yost: Well, at least with anti-virus software, Norton and Network Associates are strong bRANDs.

Parker: That was a discreet product because there was a specific add-on need, and so they survived because of that. I would guess that the next few years we will see those discreet products go away. Nobody likes security, nobody wants to buy a security product, and so they're going to buy ultimately a computer without knowing that there's an operating system in it. And in it also will be built-in the security. Everybody in the security field keeps preaching, "You gotta build it in at the beginning, you can't add it on later." And it's true, it doesn't work by adding it on later. Even the anti-virus software, you've got to get your updates every week to keep up to date and at the same time you don't want to know it's there and you certainly don't want to know that it's in any way subtracting from the performance of the computer that you're running. And the way to do that is to hide it in other products, and try to make it as transparent or at least diaphanous, as we say, as possible, because everybody hates security, nobody wants it. I hate that thing sitting in there, but it saved me, I'm sure many times, even though many times I don't even know it. The anti-virus people would love to put out a big scream every time it saves me from a virus, but they know that I am not really interested in being told the traumatic news that I had a virus and that it was successfully dealt with. All I want to know is that any viruses I get are dealt with, but please, you don't tell me about it, I don't want to know. It took a long time for the computer security industry to figure some of these things out.

Yost: And you think the major players in the industry now see things differently?

Parker: Yes, and of course what's happening right now, like this year, is a huge consolidation and a standardization so that the security products can work together. And the big exciting new thing now is the security management package that manages all the different security packages that you've got. So instead of having ten or fifteen different security packages in your system, all you see, or the systems administrator sees, is the one monitor security manager that is managing all of the other security packages. And that's happening as we speak. There will be fewer and fewer of the little companies succeeding for very long. They may form, but they'll immediately get absorbed into the three or four or five big companies that will gradually take over the whole industry.

Yost: Do you know who at IBM was the technician that led the RACF project?

Parker: There were the technologists who created the RACF, and I don't remember who they are, but Bob Courtney is the single most visible and historically famous computer security specialist at IBM, who I'm sure played an instrumental role in the design and function of RACF, from the point of view of advising what the customers are going to be wanting and willing to put up with. And Harry DeMaio, who recently retired from Deloitte and Touche, actually succeeded Bob Courtney, and another key player, Bill Murray. I'd say DeMaio, Courtney, and Murray are, from a historical point of view, the key people in the IBM world. All three of them went on to become major consultants in the field. They have continued to be developers of the many important concepts in information security.

Yost: And outside of IBM?

Parker: In the national security world of the military and NSA, Dr. James Anderson is a full-time consultant to NSA and is certainly one of the originals so he continues to be a major influence on security in the NSA military. Stewart Katsky, who I think is not retired yet and is still at NIST was also one of the original National Bureau of Standards guys. NSA was forced to work together with NBS in the development of government computer security standards that developed the "Orange Book" and then the "Rainbow Series" of books. It was mostly done and run by NSA because NSA had all the money, and NBS had a very small staff and very limited budget. They tried, with some success, to provide their capabilities and services to the U.S. business world. One of the big problems is that there is no such thing as U.S. business world; business is, by nature, international, and NBS could only deal with U.S. companies. And I said, "Well, who are these American companies, what is U.S. national business?" and they couldn't define it. They'd say, "IBM?" And they've got foreign nationals on their board of directors, that is a totally international company. "How about Unisys or Citicorp, or any of the Fortune 500 companies?" They're international and NBS and NSA were having to deal with this problem of defending U.S. national interests and then going out into the world and discovering there's no such thing in the business world. From a security point of view that was critical that national interests would be recognized. The legislators, Ribicoff on privacy and Leahy and Nelson and some of these others, all they could see was national. Even Willis Ware, a very international kind of guy always had to stretch himself beyond his U.S. Military work.

When the Internet came along it just utterly destroyed any concept of a national security interest. Then homeland security came along after 9-11 and we reinstated the concept of nationalistic information security. But with no customs and borders around the Internet, they are in a total dilemma in that regard. My approach is always international. I formed the International Information Integrity Institute, I-4, which is a commercial venture I developed in 1984 and 1985 to provide confidential advisory services to large international companies and large governments. We ultimately had seventy-five, at times eighty-five members. They paid a yearly fee to participate in this service. This was a way for me to develop sharing of confidential information among businesses to establish what I call "the baseline of information security" which ultimately became the British Standard 7799, as it's called, and the new ISO 17799 collection of information security controls and practices. I-4 is a continuing commercial service and has continued to be very successful. It got us through a couple of recessions, because information security suffered severely in the 1980 and 1990 recessions.

Yost: So I-4 became part of Atomic Tangerine?

Parker: I formed it at SRI and then SRI Consulting, a subsidiary of SRI took it over, SRI Consulting became Adario, and then Adario became Atomic Tangerine, and then Atomic Tangerine was acquired by RedSiren. And I've retired from every one of those organizations and I-4 has been owned and operated by each of those entities.

Yost: So I-4 now exists as part of RedSiren?

Parker: That's right. It was a unique organization, or service. There was no service like it at all until Price, Waterhouse, Cooper's accounting firm developed a competitor in Europe, but it then went in a kind of different direction so it ended up not really being a competitor at all.

Yost: Has it continued to grow and bring in more clients over the years?

Parker: Yes, I used to have to sell memberships in I-4, and by about 1988 I didn't any more because we had a waiting list of companies that wanted to belong. Those that did belong required that we not have more than a certain number of members. And so it limited the growth in number of members in I-4. It has suffered in the recession a little bit, but not much because it's kind of a secret club, in a way, of its member organizations. I can't talk about it very much because they don't want to be identified and it goes back to this constraint on our field of confidentiality where you do not tell others who don't need to know the details of your security. It violates security to do that.

Yost: Is it – and maybe you don't want to answer this but – is it broken down into committees that work on particular issues or industries?

Parker: Well the industries have found great commonality as far as the need for security is concerned. Banking thought they were pretty unique in the kind of information

security they needed; and manufacturing companies thought they were pretty unique in their needs; the petroleum industry, they had special geologic data with very unique security needs. And through I-4 they all discovered, "My gosh, almost all of what we need for security is common to all of us." There's very little special needs. Giant international corporations, the packaged goods industry or auto manufacturing, within those large corporations they have complete banks; they have money management; they have credit unions. And the banks discovered they've got payrolls and they've got inventories just like the car manufacturers do. So they discovered, from a security perspective, that they have a great range of common security interests.

Yost: Does it tend to be larger corporations that are in I-4?

Parker: Yes, it's among the Fortune 100, but there are some large but not super giant corporations that are involved and we do have some governments, not only the U.S. government but other governments that are members of I-4 as well. As I say, to a great extent it is run by it's members. They tell us what research they want us to do, what questions they want answered, how many members we should have, whether we should have certain companies as members or not, and so it's quite unique in that regard.

Yost: So in the waiting list it's not a matter of necessarily taking the next one but has to be a priority industry, or appropriate firm.

Parker: That's true, yes. From the very beginning there's never been much money in information security from any aspect of it you can imagine. In the very beginning information security started both in the military, in one area, and in auditing. We did the first major study of information security, SRI did, for the Institute of Internal Auditors. It was called the "SAC Reports", The *Systems Auditability and Control Reports*. I think in 1978 we did the first one and then we did a second. The audit world, some part of the audit world, realized that they needed to audit automated business processes. At first their concept was auditing around the computer; all they had to look at is what went in it, and reconcile it with what came out. Inside was a black box, they didn't have to deal with that. Gradually they realized that it was playing a bigger and bigger role in business organization and they actually had to audit inside the computer and that was very tough for them to accept because they were not computer technologists. And so a new profession developed of "EDP Auditor", who was usually a computer technologist who learned something about auditing, but in some cases auditors became computer technologists. In fact, a whole segment broke off from the Institute of Internal Auditors and formed their own audit professional organization, "EDP Auditors Association". For years we saw this splitting off and we worked hard to try to bring them back together again, but they had gone too far in their own directions and never really came back again. But the Institute of Internal Auditors was able to get some major grants from IBM and from other very large companies and contracted with us to do this major SAC study. We looked at fifteen-hundred businesses around the world and compiled all of the controls and practices that we found, we found three hundred of them, and documented those in the System Auditability Control Reports, the first study that was done. Then later on I

was paid under a grant from the Department of Justice for doing this computer crime research, but they also let me write a manual on computer security techniques in which I surveyed seven different organizations using computers and documented 82 safeguards that they were using that they all agreed were common. They all had them, they all said they needed them, and they all agreed that any organization using computers would have to have these 82 base-line controls. And so I documented these controls with two or three pages for each control and we used that in our consulting process and offered it to the world as being the base-line of information security. You either had every one of those controls or you had some kind of documented good business reason for not having one of those controls. Shell International adopted those as its policy that throughout the world Shell must have those controls in place. And then they offered those controls in a committee effort done by the British government that resulted in the British Standards Organization, 7799 Information Security Controls. They expanded on it, and it became their primary set of information security standards. That has since expanded and the International Standards Organization is in the process of adopting that as their ISO standards. More and more, I see in the trade news, there are more efforts now to pool information to identify what are the required controls. Because now we've got GLBA, the Gramm-Leach-Bliley Act, and we have the Health Insurance Portability and Accountability Act (HIPAA) in the health field, and the "S-O" Act – The Sarbanes-Oxly Act that requires the owners and management of firms to sign their names to the accuracy of the accounting. That requires also, a set of generally accepted controls and practices. So looking at that with the idea that this is ultimately, finally replacing the whole concept of choosing controls based on risk assessment, which was suppose to be the preferred

method of choosing controls and practices, and I've claimed for many years it doesn't work, it's too expensive, it's impractical, we don't have enough data to back the calculation of risk Forget risk assessment and risk management and adopt the generally accepted due-diligence practice as your objective in information security. It is more important that an organization has in place the generally accepted controls and practices, or positions on them, than it is to try to argue that they've got some kind of risk reduction because they can't prove risk. But they can prove that they are meeting the requirements that are now being gradually applied by HIPAA, GLBA, and these other requirements. First, 7779 and the GASSP principles of information security that ISSA has developed, and the ISO are all moving towards the due-diligence, generally accepted controls and practices. So ultimately I think I'm going to win, but it's still a battle between me and the quantitative risk assessment people who think you can apply mathematics and history to computer crime, and you can't do it.

Yost: You mentioned some key figures in security that I should speak with or perhaps interview?

Parker: Yes, we were talking about who were the key movers. These are people I know, there are lots of highly qualified people that I either don't know or can't remember the names of, so what I have to say about it really is biased. Robert Jacobson, an independent consultant in New York City and Robert Courtney are the two that got the U.S. National Bureau of Standards (NBS) interested in risk assessment concepts. They and I continued to be in different camps on this subject. But Jacobson and Courtney had

a great deal to do with the initial development of information security. Jacobson stayed out of the limelight to a great extent and has been a very successful and competent security consultant. Drs. James Anderson and Willis Ware, and William Murray come to mind as pioneers.

The major annual conferences, the RSA conference – the biggest one now – along with Computer Security Institute Conferences that have been running for twenty-five years started with three or four hundred people in attendance. Today five thousand people are attending RSA conferences. And then there are the hacker conferences that makes the criminal world look totally confusing. I mean that, in the past there were good guys and the bad guys; and the good guys and the bad guys were at war. Now they all attend the same conferences.

TAPE 2 (Side B)

Parker: The juvenile hackers are trying to do something so outrageous that it would be noticed, so that they can ultimately get a high paying, hero-type consultant job in computer security. It's thrown the whole good guys- bad guys world upside-down. The bad guys hold Black Hat and Defcon conferences in Las Vegas every year. And the criminal justice people can look on with horror, but they go to them because they want to identify the criminals that they're going to try to arrest, convict, and put into prison. And there they all are, kind of milling around together: information security people, even such

companies as IBM offering consulting services called “ethical hacking consulting services.” I mean, come on.

Yost: They’re recruiting even?

Parker: Well, I don’t know. But they’re offering bright , eager, young, technologists to come in and hack your systems for you and tell you where your vulnerabilities are. And they’re called ethical because the IBM name is behind it and it is certainly ethical practice that they carry out. They use the word “hacking”, which the news media has totally corrupted to be a totally negative term for somebody. Which it turns out shouldn’t be that way at all. I always referred to hackers as either “hackers” who are not malicious, or “malicious hackers.” And it’s the malicious hackers who are enemies that we’re trying to deal with. But separating out hackers from malicious hackers is difficult. One day a malicious hacker is a hacker, another day a hacker becomes a malicious hacker depending on what gang of kids he happens to be associating with at the present time. And it’s all mixed-up; it’s extremely difficult to separate it all out. Now, malicious hackers, some of them have become career criminals; they’ve entered organized crime and they have real criminal careers. Some of them are trying to overcome their past backgrounds to get legitimate jobs in information security or computer technology. And then others have simply gone off into other professions. But it does present a very unique problem because it’s ten and twelve year old kids who are getting sucked into the malicious hacking culture and causing tremendous damage because of the huge leverage they have with computers. They would otherwise be running around doing graffiti or

pushing over “port-a-potties”, as kids pranks, now they’re doing kids pranks but with this tremendous leverage and they have no idea of the billions of dollars of losses that they’re causing. It is a particularly unique problem in society today. And it’s not been very successfully addressed; you can get strong laws and put hackers in prison for ten years and that’s being done, but that’s a sad solution to a juvenile delinquency problem which is what malicious hacking, to a great extent is.

Yost: Do you see any other possible remedies?

Parker: I’ve tried to do some work in this area trying to get to the ten, twelve, thirteen year old kids, in middle school and high school. And give them a dose of ethics and responsibility along with the technology that they are learning, and try to find ways that they can express themselves in non-malicious ways. The FBI has had a program to try to do that as well. I’ve been trying to interest the communication companies and large computer manufacturers to try to come in and support that kind of activity, although I haven’t been particularly successful except for here and there on a very small scale basis, nothing sufficient to meet the challenge that we face today.

Yost: I think I mentioned in my email that we’re very interested in doing a history of computer security and privacy study at the Charles Babbage Institute. I very much appreciate you giving us your collection of materials.

Parker: My collection of computer crime cases really developed in 1966 when I started collecting them. And I think there must be over four thousand cases. Unfortunately only part of it has been indexed. We ran out of money and we had to seek our funding for work from other sources that didn't allow us to do that. But as a side thing I found the time to collect them and had a clipping service that worked quite well, because we had it for so many years. We had little old ladies sitting in apartments all over the world clipping news articles and they knew what to clip because of the experience in doing it for a long time and the feedback that we'd given. So we've got a pretty comprehensive collection, I can't say complete, but I think that collection of computer crime cases is a valuable resource.

Yost: The cases, I believe, started in 1958, was there an effort to go back further or were those the first articles you found on computer crime?

Parker: I tried to go back further, but further back than '58 I ran into punch card systems that actually were used in business environments in which crime could happen. The earliest cases were mostly violation of trust kinds of crimes, because nobody outside had any access to the computers, it was all inside. So it started out that way and there were big arguments at that time about what was a computer crime, and I defined it very broadly because I wanted to include any kind of crime in which there was something to learn that we could apply to the protection of information in computers. So I didn't care too much if you wanted to argue whether something was a computer crime or not. My criteria was, "Can we learn something?"

My gRANDfather engaged in a bank fraud in 1912 in Winnebago, Minnesota; his crime was discovered the same day the Titanic sank. In family research I went back and studied his crime, and he was trying to help the local farmers save their farms in a severe recession. He was mayor of Winnebago and vice-president of the little three-man bank, and violated banking law because he gave these loans out and he shouldn't have. But he kept it secret and hid it from the state bank examiners. He had a secret way of knowing when the bank examiner was going to come to his bank. So he cooked the books to prepare for the visits. One day a new bank examiner showed up and surprised him. By studying that crime in great detail and then applying it to all the other crimes, I realized that an extremely important aspect of crime, for security purposes, is predictability. Criminals need to predict the exact circumstances and environment of their crimes, or they will be caught or their crimes will fail. So predictability is a critical factor in all crime. And now applying this factor gives us a very powerful capability that we have hardly used at all, and that is to make computers predictable for approved use but unpredictable for malicious use. And it can be done in lots of different ways: there's an attack called the "buffer overflow attack" where you send more information into a buffer as input than the buffer is able to hold and it spills out into another part of memory where there are either programs or data. You can insert your own code or data into a secure part of memory and therefore take over the entire operating system this way. Well, if you apply the concept of unpredictability, if you design the system so locations of code and data are not predictable, just outside of that buffer, you've destroyed the buffer attack. And it turns out, I just learned last week, there is a company called BSDC,

it's a joint venture of a lot of people in developing and providing a specific version of Unix, that is now designing this software so that it RANDomly places pieces of the operating system and data so you do not know what is beyond the buffer, and it's not possible to predict. That's just one little example; making passwords of variable lengths so you don't know how long the password is as well as what it's content is; developing time-outs and transaction floor limits that are created by RANDom number generators so that no human knows what the time-out is and no human knows what the current floor limit or transaction limit level is above which you audit each transaction. Those are again some simple examples of building unpredictability into systems.

Another great concern that I had that I have seen from a historical point of view is what I call automated crime. We automated business processes, there's no reason why criminals can't totally automate. So for the first time in human history it's now possible to possess a crime. I can hold a disk in my hand that contains a crime. So no longer do we need to think of crime as something that's done one-up; you do a crime, one at a time the way we used to do business processes manually. We now possess business processes; I can hold the complete Turbo-Tax in my hand, a complete business process, or an inventory system, completely in my hand. And so we buy and sell business processes. Well now you can automate a crime so that the selection of the victim, carrying out the crime, the erasure of all the evidence, and the conversion to gain, are all done in a complete single software package. I have some scenarios of how the complete crime is all in one single package. So you can buy and sell crimes: go into a store and say, "Here's an inventory fraud, $39.95." or "Here's a colored box that says 'payroll fraud', $29.95." It's not quite

that, but the criminal world is going to automate and is going to go into the business of selling their crimes. So crimes are not just done once, and then it's all over with, it's done once to develop the crime, again to further it, and ultimately have a complete automated crime for many people to execute many times.

Yost: The ones that work best continue to sell?

Parker: Right. And I'm beginning to see the sophistication of the security tools that are being developed, starting with SATAN, which was kind of the original well recognized, tool that you could send out on the Internet and it would come back to you and report on all the vulnerabilities that it found in all the computers you told it to look in. Well, all you have to do is take the reporting end off SATAN and put the crime end on to it, send it out into the world, and it finds the computers with the vulnerability, and it finds those computers, for example, that happen to have a certain accounts payable package in them, it then goes into the accounts payable package, sends $34,000 out in a funds transfer through the Cayman Islands to a criminal bank that then funnels the money back to the perpetrator, and you have the perfect crime. Because you've been able to develop it a step at a time and test and improve it, the perfect crime. And it erases all of its evidence of having existed, you do not know where the money went and it simply ends up in the perpetrators account. And the perpetrator does not know what crime was done, does not know who the victim was, does not know anything about the crime except his account seems to have $34,000 more than it had yesterday. You can download this crime into your computer, execute it, and then when you go to look for the crime in your computer

it's gone, it's not there anymore, it doesn't exist. You go back to the Web site where you got it and they've changed so that there is no such thing as "fraudster computer crime program" anymore.

Yost: And that's occurring today, or not?

Parker: I'm seeing this , as I say, gradually develop historically with more and more sophisticated tools of this nature, and with sophisticated worms and Trojan horses and viruses that are now blended, where they are putting multiple methods of attack in multiple payloads that will do lots of different things in a single attack program. These are all gradually getting more and more sophisticated just like we did with automating business processes. I predict in the next several years we will certainly have a completely automated crime. I checked with some people who handle illegal funds transfers in Barbados and various places where people hide their money for tax purposes, and I've shown them my scenarios and they say, "Absolutely, that will work perfectly." Where it is not possible to connect the money you have gotten with its source. And I think we're going there very rapidly. So we shall see.

Yost: Is unpredictability the best tool that can combat automated crime?

Parker: Right, if you can make a system unpredictable then you've destroyed the automated crime. Because it has to know where every bit in that system is.

Yost: But if it's going out to a whole bunch of different systems, it will probably find a valid match.

Parker: And of course a problem with security right now is that we've got lots of great security packages and the industry is providing them. But still the world is hugely vulnerable to computer crime because there are still hundreds of thousands of computers that do not have the protection and have not paid the price for that protection. You cannot prove the integrity of the software we all use. You can prove that it will do what it is suppose to do, but you cannot prove that it will not do what it's not suppose to do. And the complexity of systems is growing far faster than anyone will ever be able to produce the tools to assure that you do not have more attack vulnerabilities. So security will always be imperfect. If you consider the amount of money and of people and of locations all being shoved closely together electronically on the Internet, the potential for crime is just unlimited. I've noticed over the past thirty years the size of loss in individual business crimes of all kinds has grown dramatically, not because of inflation, but because of the automation applicable through computers. Electronically it's as easy to steal a million dollars as it is to steal $100. So that's certainly been one of the changes in business crime that has occurred with increasing use of computers. At the same time, computers are ideal targets for those who have the technical skills and the knowledge. And they are totally uninteresting targets to those who do not have the skills and knowledge. But we have enough people with the skills and the knowledge now so that computer crime will flourish. Computers don't cry, they don't squeal, and hit back when you criminally attack them. And there's a satisfaction and an anonymity attached to it.

Yost: It's crime at a distance.

Parker: Right, and with computer communications we have removed the need for proximity to the site of your crime. So you can do a crime from a telephone booth or someplace in any other part of the world now. This is requiring cooperation among the world's criminal justice community that has never been before. And there are efforts going on now trying to do that. Letters and other means of getting cooperation agreements among the criminal justice agencies in different countries. Of course that's been stimulated by the terrorists, a separate issue , but it has its purpose in the Internet and computer fraud as well. The history of abuse and misuse of computers, I have found, is totally fascinating to see what people did in the early days of computing and how that's evolved into malicious activity going on today, and still with the same old objectives of solving personal problems. The challenge of that for computing is really tremendous it. And people are questioning the future of the Internet; Spam alone is threatening the future of the Internet. A lot of the solutions are resulting in restricting of civil liberties, where that seems to be the only solution. The contention between preserving civil liberties and abrogating them sufficiently to catch the bad guys has never been more intense than it is today. It's hard to know where that's going to go. Everyone's worried about the issue of privacy; identity theft is the number one theft in the United States now. Where privacy is going to go and what I've seen in the past forty years or so is something that I don't think that's been taken in account; the concept of what is private is changing dramatically as well. It used to be that your annual income was one of the most private

bits of data that you have, and it used to be that having cancer was the most private piece of medical information that you could possibly have. And now having cancer is public knowledge, and your annual income is not quite there yet, but certainly moving in that direction. There is an openness among young people today in sharing their sexual problems, in sharing all kinds of problems that ten or twenty years ago no one would even think of revealing to other people. The trade off that you get, "Wow, if I give my social security number I get all these goodies back." Or "If I get passport through Microsoft, or the AOL "Paypal" service, I can give them all my details, credit card numbers, information about me, and it will be so much easier making transactions, I'll get all these wonderful things in return." In the mean time of course, I've lost my privacy and I've put myself at much greater exposure to the possibility of identity theft. So what privacy issues are, what we're trying to keep private is different than ten years ago. Where's it going to end? With universal identifying numbers embedded in chips under our skin? Well, they're doing it with dogs, how soon, before they do it with humans? They'll do it when what you get in return is of a big enough advantage. So the commercial world is going to win in the long run. Putting these cheap RFID chips woven into clothing now, and these chip transducers are going to be inserted into every product we have, so that every single product can be electronically tracked exactly where it is and its conditions as well. We've already done that with OnStar Cadillac Service so that the Cadillac Corporation knows exactly where every Cadillac that has the OnStar service is, and what condition it's in. Everyone is saying what a wonderful thing that is, "If my car is ever stolen, no problem, Cadillac will find it." Well, Cadillac will also know exactly where I am.

Yost: How does it monitor the condition?

Parker: There's the microprocessor, cell phone communication, and GPS, it knows exactly where the car is and reports that. But that microprocessor is connected to the processor that runs the engine, and I think there's six microprocessors together that run the engine, and all of your instruments. So it has access to the whole thing. So it can tell you, "Hey we've got about 40,000 miles on these tires and you ought to come into our shop to get those replaced with our better tires."

Yost: A scary thought.

Parker: Then you add to all these scary things that are happening, the criminal world, the malicious side of the world, and from my Christian values every person is fundamentally bad, sinful – boy, the mix is kind of exciting. So we shall see. At the very least, we've got to capture the history of it all. While most people in the computer field don't like the idea of their world being invaded by bad people, it is, and we have to document that it has happened and it is happening to convince people that they need to establish systems with rewards and penalties to motivate people to protect not only their own information, but their employers information as well.

Yost: Well, this is a fascinating topic, I really appreciate you taking the time for this interview.

Parker: I appreciate the opportunity and I'm hoping that being associated with the Babbage Foundation will be helpful. Ultimately, I'd like to see a history of the computer and information and security field accomplished, especially before some of us old guys pass on. I'm hoping that I can help find the funding and generate the interest so we can do that.