An Interview with

JAMES BIDZOS

OH 376

Conducted by Jeffrey R. Yost

on

11 December 2004

Mill Valley, California

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

James Bidzos Interview

11 December 2004

Oral History 376

Abstract

James Bidzos begins by discussing his early career at IBM and as an international businessman in IT. He then moves on to describe how he came to take the helm of struggling software security firm RSA Data Security. He relates a number of early business challenges in financing and technology at this firm as it sought to commercialize encryption technology that extended from the research of MIT's Ronald Rivest, Adi Shamir, and Len Adleman—work that in turn built upon the invention of public key cryptography by Martin Hellman, Whitfield Diffie, and Ralph Merkle at Stanford University. In discussing how RSA developed into the leading software security firm, Bidzos describes the challenges posed by the government's attempts to control the dissemination of encryption technology through export laws and other means. An important forum for debate on such issues (and later issues like the Clipper Chip) was the annual RSA Conference, a meeting that Bidzos initiated that included individuals from industry, government, and computer scientists, and evolved to become the leading annual event in the computer/software security field. Finally, Bidzos discusses the commercialization of encryption for authentication (signatures) by partnering with other major firms to found VeriSign.

TAPE 1

Yost: My name is Jeffrey Yost. I am from the Charles Babbage Institute and I'm here today with Jim Bidzos at his home in Marin County, California. It's December 11th, 2004. Jim, can you begin by talking about your first job in computing a little bit? That was at IBM as I understand it.

Bidzos: Yes, basically I sort of fell into writing computer programs. And later I got a job at a bank that was on its way to becoming a big IBM customer. IBM liked to put people to work where they could help sell equipment. I ended up working on a very large project at a major retail company called Federated Department Stores, which was the owner of a lot of department store chains. In the late seventies, Federated was doing something very interesting, it was building one of the largest private networks anywhere—one of the first large IBM style networks. The architecture was called SNA, Systems Network Architecture, which was IBM's way of doing networking. It had this massive project to put about a dozen of IBM's largest mainframe computers in a room, in Ohio at its headquarters. It would use these new distributed computers, called the 4300 system, in all of its twenty or so chains that it owned. It basically wired all of these things together so it could get what people take for granted today: a screen or a piece of paper that provides everything that happened in all of the corporation's business operations yesterday. I got involved in being a systems programmer and making all the software work. That was an interesting, exciting, big project. In fact, one of the interesting things I remember about it, and I never even thought about this until recently, but it's a strange, funny kind of connection, one of the senior executives actually said, “What happens when we transmit all of this information from the stores back to our headquarters, couldn’t somebody intercept it? Isn’t it vulnerable?” We said, “Yes, I guess we could scramble it.” So, I wrote some very rudimentary [code]—actually it turned out to look like a one time pad. It was just basically a key used to exhort data. The key was actually embedded in the data stream. We figured that nobody would ever figure out that we were thinking about this, much less realize that we had actually embedded a key in a stream of equipment data. We did all that to make this guy feel better, but it was just interesting that that is what happened. At the same time, I was sort of a computer hobbyist. There was something called the Western Digital WD90 Pascal micro engine that was basically an interpretive Pascal computer that didn’t have a whole lot of stuff working for it. A guy I worked with—and again this is an interesting connection to what came later—had the great idea to develop a bunch of business applications and sell these to everybody. This is I think around 1979/1980. He had decided that he would develop a lot of the tools that business programmers would need to write the business applications. That, in turn, would lead to the sale of a lot of machines and make him a lot of money. So actually what he specifically had me help him do, or write for him, were some routines that would allow large integer arithmetic to be done on these computers. I had no real awareness of what was going on. Actually, at about the same time, this whole business of public key cryptography, that’s sort of a related kind of thing, was going on. Around this time I went to work for another company. I think I got a taste of the entrepreneurial bug in a funny way. These people from a company called Paradyne were coming to Federated to sell us equipment and they said, “Oh we’ve got a much better way to do this networking thing.

We have this much more efficient equipment that doesn't require all this complexity and cost that IBM requires. And here's how it works." I was really intrigued by it. I thought, "Wow that's really clever, that works great." The problem is in order for this stuff to work, it gets really close to some of the inner workings of the operating systems on these large IBM mainframes, which was fine because I understood that stuff pretty well. I understood exactly what they did and I realized that it wouldn't be any kind of problem, and it would work well. Needless to say, the IBM people were not really happy about this alternative equipment being considered. I was entirely naïve. I had no idea what sort of political and economic battles were actually being waged here. I just thought this was really kind of interesting. So I suggested we should all just get into a room and figure this out together. I thought we should get the IBM people and the people from this other company together in a room and I could explain to them why this isn't so bad, that IBM really doesn't need to be worried about this, not realizing that this was not what they wanted to do. So, I actually refuted all of the claims that the IBM person made about what a bad decision this would be. And I did that so effectively that these people said, "You know, you could be very successful working with us. If you could just repeat this performance say twenty or thirty times a year, there would be a lot of interesting things that could happen as a result of that." I ended up going to work for them. That was an interesting experience, during the four years or so that I worked there that company went from perhaps less than two hundred employees to about twenty-five hundred employees and from something like fifteen million dollars in annual sales to almost three hundred million dollars in annual sales. And this particular product that I was specifically working with went from nothing, from less than a million dollars in annual sales, to accounting for maybe thirty percent of all of the revenues of this company, which also made network management systems, modems and multiplexers, centralized management systems, and other products. That was a very good experience. I definitely had some of the entrepreneurial bug. I had risen in the ranks in this company and I had a lot of responsibility for several product lines, all associated with networking. There was a fellow that I worked with there who I got to know pretty well and he really wanted to be an entrepreneur. He recognized that I was moving in the same direction. We both left the company. We chose different paths that later converged about two years later.

Yost: That's Bart O'Brien?

Bidzos: Yes, that's right. So I went off to work with some other people in an international marketing business. I just thought that it would be cool to be an international businessman. I can clearly say that I had absolutely no idea what I was doing. But the idea—I actually do remember one specific instant, it became pretty clear to me. I don't think it's a composite sort of thing, I think it actually happened in a span of a few seconds on one occasion when I watched an airplane going by and thought you know there are people in there, in that plane, flying in the first class cabin going off to some exotic places to meet interesting people, and do deals—whatever that meant, it sounded pretty cool. So I thought I should do that. And so I did. And after a couple of years of doing it I realized that that's an interesting business, you meet a lot of people, you travel a lot, you get really tired, you're only as good as the last deal that you've done, and there's no real equity in it. About this time I reconnected with Bart O'Brien. If you think of RSA at the time as these three professors who bought the company in 1982, I came to them through O'Brien who came through somebody who was in the venture capital business who referred him. The venture capitalist dropped the name RSA and mentioned that there was a guy named Ralph Bennett who came to RSA via the first investor who was a medical doctor from Reno named Jack Kelly. And so the three inventors somehow found Jack Kelly who put up some money, and Jack Kelly found Ralph Bennett, who was the first CEO. Ralph Bennett somehow connected with Bart O'Brien. I came to visit Bart in California sometime in 1984 or 1985.

Yost: What was Bart O'Brien's position?

Bidzos: Oh, he was one of the principals of the company. You mean at RSA?

Yost: Yes.

Bidzos: Yes, there were only two or three people that worked there—so I think he called himself whatever he needed to at any given point in time. So my first involvement came about because Bart asked me to help him…Basically I ended up writing a strategic report that stated, "Look, here's how you can apply this technology in a way that would address some of the security weaknesses that exist in these IBM networks. Here's how this technology could be applied." That's how that started. Bart was obviously struggling somewhat, he wasn't getting along with Ralph, the company wasn't making any money, it had no money. It raised a little bit of money from a very interesting investor group from

New York. This is one of the so-called investment banks that seems to be two guys, one cell phone, and an address somewhere in Manhattan that changes frequently—I'm not exaggerating. Even the name—I won't use the names of these people—but their names even sounded like characters out of some really bad novel. They were just caricatures of themselves, they were really interesting characters. At any rate, there was some money that had been raised from these people and that money had pretty much been spent, back salaries, loans, all of it just kind of disappeared. So there were no real prospects of anything happening. I think Ralph Bennett just really wasn't a businessman. I think he didn't understand what was going on. I think he just hired Bart to try to go sell something and drum up some business. I think Bart was entirely inexperienced and unrealistic and just didn't understand how to do deals. At least I'd learned something in the last few years about doing deals. It became pretty clear that the company was in trouble. I was in the process of moving to California at the time. This all sort of came clear in late 1985 and early 1986, things were kind of falling apart, to make a long story short.

Yost: With the marketing?

Bidzos: With pretty much everything, with the financing and marketing, and in fact, the technology too. In 1982 Rivest, Shamir, and Adleman decided that the right thing to do was just to build a RSA chip and the world would beat a path to the door and everybody would want it. There would probably be all kinds of cool things they could stick it into later. And so they taught themselves circuit design and went about building a chip. And they never quite finished it. It didn't quite work.

Yost: And the marketing enterprise that you had started, how was that going?

Bidzos: Well, I don't think it was going at all. I mean it would take money—you're talking about this thing I prepared for Bart? Or later?

Yost: Actually, moving a step back, I am referring to earlier, to the international marketing.

Bidzos: Oh, the international marketing, doing deals.

Yost: Yes, I'm interested in the transition for you.

Bidzos: Oh, O.K. So the transition was the realization that this is too hard, that this is too demanding, this is too difficult, that you're only as good as your last deal. You're building a lot of relationships but they're only good if you work them.

Yost: Was all of this international marketing work in the IT field?

Bidzos: Yes. The pitch was that I would go to a new start up computer company in the United States and say, "I'm your international marketing department. You can hire somebody for a lot less than you're going to pay me who might learn to say, 'Where's the bathroom?' in some language after a year and come back and do nothing." I said, "I'll go out and tell you what you've got. I'll tell you what the potential for your product is in different markets outside the U.S. At this point the overall market for any given company was still heavily, heavily lopsided in favor of domestic business. Now it's different obviously, most people get a majority of their revenue from outside the United States. But that wasn't true at the time. I was helping people with that transition. "Hey, plug right in. I know all the distributors." I'm reminded of that scene in one of the Indiana Jones movies where Harrison Ford says to his captors who want to get a hold of a guy who's got a book with a map in it or something. And he says, "You'll never find him. He's disappeared into this country with these other people. He speaks twelve languages, he knows all the customs, he's got connections." And then there is a cut to a scene where the guy's lost and he's wandering around looking very much like a tourist, begging somebody to please identify themselves if they can speak English. So in a sense I think I was maybe a little bit like that, not quite that bad, but at any rate I definitely understood the marketing and the technology, and I'd run around the world and started hooking up. I went on a couple crazy trips where I just met with everybody who'd meet with me who was a distributor. For example, I found a company in Taiwan that made really low cost IBM compatible terminals and I started feeding them into the German market through a big German distributor. And that turned out to work pretty well. I did the same thing in France and used trade-free zones to even re-label some of these things. It was interesting stuff. It was fun. I did what I wanted to. I traveled to foreign countries, I visited exotic lands, I met interesting people, I stayed in hotels, and learned a lot about food and wine—and I did deals. You can only do so much of that I decided. You burn out. It just didn't seem like a good way to build much equity. One of the clients that I had was a company that was in Southern California. Its products consisted of a family of fiber optic communications devices. The owner of the company, I think kind of liked me, and I kind of liked his secretary, and I think he knew it. I had dinner with him whenever I visited and he sensed that I was getting tired of what I was doing. He said, “ Look, why don’t you come out here and give me two or three days a week.” He said, “You probably want to move out here anyway and if you give me two or three days a week, I’ll pay you this much. And you can take a break or wind your other business down or decide whatever you want to do.” But he created some nice options for me, so I took it. It was early in 1985 and I spent about a half a year or so living in Southern California. And I think that’s when I did some preliminary work for Bart. So in very early 1986, Bart said, “Come up here and help me do this.” I didn’t like working for the fiber optic company, I’d broken up with the secretary and fiber optics just didn’t look like a really interesting thing to do. The distributor network they had in the U.S. that he wanted me to nurture and build was really boring. I just found it all incredibly boring after what I had been doing. So Bart convinced me to come up there and work with him, and so I did. At that point it became clear that…let’s just say that I don’t think anybody knew how bad things were until I got up there and started spending everyday sitting down with Bart saying, “Gee, this is really bad. You’ve got a real, real problem here.” There’s some other very dark aspects of this that probably are not appropriate to go into, having to do with some of the other people who are on scene at the time. Some of it troubling and maybe even dangerous, but that just sort of added a little bit of excitement to all of it I guess. So at any rate, what happened is that I pointed out to Bart that this whole thing looked like it was just about to go broke. I don’t think Ralph Bennett was aware of that at all. Rivest was definitely not aware of it at all.

Yost: Of Rivest, Adleman, and Shamir, was Rivest the most involved in the company?

Bidzos: Well, Adleman had called himself the president…I think Rivest was the most involved when I got there. Actually, I think up until that point, none of them were that involved, Rivest more than the others, but none of them were really all that involved. They got involved in the chip design. So at any rate I don’t think that Ralph Bennett…they just all seemed oblivious of the fact that the company was in trouble—it was obvious to me because I had just spent a couple of years doing things on my own. They fooled themselves about reality in terms of whether money was going to roll in, and were unrealistic about how much things cost. I was painfully aware of all of those things. I had to be. It just was clear to me that they were oblivious to all this. They had raised some money from these people in New York and they had pretty much spent it all. There were no prospects of selling anything to anyone. There really wasn’t anything to sell. There was no prospect, it seemed to me, of raising any additional money. There were all these wildly optimistic ideas, forecasts and thoughts about what might happen and who might give us money and that certain people are going to invest. I talked to somebody in AT&T who said, “This is important technology to have and I think we’re going to get ten million dollars for it.” “Oh, who was this guy?” “Hold on, here.” “This says Assistant Systems Analysts. I don’t think so. Does this guy make decisions? Does he have any kind of budget authority?” “Well, no, but he really likes the stuff.” “OK. Scratch that off the forecast, I don’t think that’s going to happen.” So I told Bart that we really needed to explain this to Rivest because there are probably going to be a lot of lawsuits. These people in New York don’t seem very friendly and they seem really pissed off. They seem to think that you and Ralph Bennett told them some things, like you would already be public by now. They would have made ten times their money. They want to know where it is. And you know this is going to blow up in everybody’s face really, really badly. So we made a trip to visit Rivest. That was the first time I met him and we explained all of this to him. Actually laid it all out in the light for him. “We’re not taking any salaries, but you’re out of money very, very shortly here.” Rivest’s attitude was, “Well, that’s too bad. I was hoping this would all work.” And so I said, “I don’t think it’s going to end there. You’re the Chairman of the Board, you were involved in raising this money. You’re going to get sued. It’s just going to be ugly. Do you have any insurance?” He said “No, of course not, it’s just a small company.” I think at that point he started to get worried. And so that began this flurry of activity, like, what do we do. Finally people, Rivest and Bennett and others, started to realize that it just wasn’t working and that simply waiting for something, some big check to roll in the door delivered by some assistant systems analyst from AT&T, wasn’t going to happen. So I guess over a period of months the question was what to do. I think the conclusion was basically cease operations and stop spending money. That was the hardest part, getting people to just stop spending money. And then trying to figure out what the options were from there. We brought in some consultants who helped us a little bit. But I think in the end it arrived at a point where I would go ahead and try to keep the company alive at a very low burn rate, essentially by myself. So by the end of 1986 I was the only employee basically. I brought some guy in later who had worked with me earlier, and then in 1987, I actually hired the first employee. I managed to negotiate away some of the debt—the company had huge debt. It had more debt than it ever had money. There was a law firm to which we owed a ton of money. Actually I do remember very clearly having a conversation with a partner of that law firm offering, or saying, “You’re not going to get all of this money that we owe you, and I have got some options for you. I can give you some of it, or I can give you some stock.” He declined my offer of stock and I reminded him of that ten years later in 1996 when I was in a conference room at his law firm with Rivest and a bunch of other people. We were having RSA’s last shareholder meeting because we merged with another company and I just had to remind this lawyer at Fenwick and West exactly how much money he would have made if he had taken my offer. I think it would have approached a hundred million dollars for a thirty thousand dollar legal bill or something like that. So at any rate I negotiated some of that stuff away and some of the more fun parts of that were things like going to New York and meeting with these guys [early investors] for the first time. When I met with these people I was sort of in shock. I had no idea that there were really people like this. I mean I thought all business people wore suits and were pleasant and occasionally business deals fell apart and that was the end of it. I didn’t realize that people got upset and screamed, and threatened people. It wasn’t really going well with them. I don’t think they were happy with what had occurred. I don’t think they were happy with me. I said, “Look, I’m going to try to get this thing going again.” And there was one meeting where somehow, I don’t know what happened but we were at Kaplan’s Deli on Park and East 59th eating lunch. I was getting screamed at and threatened and everything else. The check came and I took the check and I paid for it with a credit card. I filled out the slip and I gave it to the waitress and then she came back and she just threw down this credit card receipt, or the whole thing, not just the receipt, the whole package. And she said, “You made a mistake calculating the total.” And I thought, “Oh my god. How embarrassing.” I was in shock. My face was red, I just kind of buried my head and I said, “I’m sorry.” And I looked at it, and I had added it wrong. I had accidentally shorted them. It was less than fifty cents. I don’t remember if it was twenty-eight cents or thirty-eight cents or forty-eight cents, but it was a few dimes. I’m looking down fixing this and I’m thinking, “What an idiot.” This lunch has been a disaster and now it’s just getting worse. And when I looked up, for the first time, these two guys were smiling at me and they looked at me and one of them nodded and said, “It’s OK. We like that.” I thought what have I gotten into? What is this? They like that, they respect me now. So I just sort of nodded. But at that point I think they were willing to, well, not do anything they had threatened to do. They were willing to just wait it out. I would find some way to make them whole. I gave them some assurance that I would do that and kind of realized that it might even be fun to sort of pepper my assurances with a couple of threats. I mean it’s sort of like discovering that you have this new weapon. If you just do rude things they react, they like you, they smile, they get respectful, they nod. Oh O.K. this is great. I’m starting to learn how this works and that was like the beginning, the real beginning, of my business education. I had a similar situation with this fellow Dr. Kelly, the medical doctor from Reno who provided the first funding. And in another scene that sticks out in my mind of going to visit people, there was another MD, an Asian MD in Southern California that Kelly had known and they both met at Pepperdine University when they were getting MBAs. MD’s with MBA’s, who continue to practice medicine and dabble in business, that is a very dangerous thing, as I learned later. But at any rate this other MD apparently he did a lot of work in the aerospace industry and made some money investing and doing some other things. So Dr. Kelly had this “great idea.” It seemed to me that his knowledge of the business world consisted of the pink slip, petty stock market, where a lot of people get robbed of a lot of money by unscrupulous people. He knew a lot of those people. And I think this other fellow was one of those too. So at any rate when we went to visit him I thought, “Wow, what an impressive office, what a great place.” This guy is a doctor, he’s actually got some sort of an engineering Ph.D. as well as the MBA. He has done a lot of great things and he has a project, a government project that maybe can utilize some RSA technology. And I thought, “Oh this is a nice thing. Kelly going out of his way to do all this.” We traveled and met down there in Southern California. We go down to the meeting and this fellow makes a very good presentation about the project and I thought, “Well, you know, there’s maybe some potential in this” And then all of a sudden Dr. Kelly gets up and takes over the meeting and starts describing how, what we should really do is form a new entity to exploit this new contract, we should merge it with RSA, then we should find a shell that’s traded on a pink slip, over the counter markets process, put them together in a merger, give ourselves a whole bunch of stock, issue a series of press releases, get some shares at a friendly off shore with the dragon lady… He’s using all these terms that apparently exist only in this world of petty stock manipulators. I’m just sinking as he’s saying this. I’m thinking I can’t believe this is happening. This is so embarrassing. I’m with this group of professionals. I think of some sort of a gangster getting up in the middle of a Fortune 500 board meeting and saying, “This is what we should do.” And I’m thinking what’s going to happen now, this is going to be the most embarrassing thing." Then when Kelly stops talking this other guy immediately jumps in and just fires off this burst of chatter that sounded pretty much like what Kelly had said, but built on it a little bit. And I thought, "Oh my god, he's one of them." I felt like some guy who had wandered into some village that had been taken over by aliens and realized now that they're all part of this, they are all aliens. It was just a strange, strange thing. Anyway I managed to survive all of that stuff and get the company going and got it built up. But those are some of the memories of the transition. I do remember those quite well, there were lots of other colorful episodes. It was an interesting transition—lots of time spent with people trying to find some way to raise that money. I'd visited every venture capitalist in Silicon Valley too. Some of them got it, some of them didn't. I totally understand why they couldn't possible invest in it, there was no market whatsoever. No addressable, actually very little definable, market. Not really much technology either. There were some good ideas and maybe some raw pieces, some tools and things like that. So somehow in those lean years of the second half of the 1980s we managed to survive. I thought several times about giving it up during that time.

Yost: In 1985 I understand Bart O'Brien and Ron Rivest met with Iris Associates, which was partnering with Lotus Development. What was the state of that when you came on board and can you describe your meetings with Ray Ozzie and the negotiations for that deal?

Bidzos: Yes. Ozzie had formed Iris Associates, was working on a project that Mitch Kapor was funding for them which was Notes basically. Ozzie decided, that they needed to have security in their program. They had done some development of symmetric ciphers, they'd done some things, and they wanted to use public key encryption. They found out that it was patented, so they came to us. I think they went to Rivest and he turned them over to Bart and Ralph. They were talking about doing something with them. Later it became helping them [Iris] do it, to develop some software to help them make it work. I think those preliminary contacts were made in 1985. There were a series of meetings in 1986. I think I might have gone to one of those with Bart. We didn't meet with Kapor. In fact he left in June or July of 1986. I remember that because I was suppose to sign some sort of a contract with him that would give us the money that would keep the company going and the day that I showed up to do that in July of 1986, he had resigned. His picture was on the cover of the *Wall Street Journal* that was in the lobby that I was looking at while I was waiting for my meeting with him. That was the exact same day. It might have been July 29th. Yes, I think it might have been. It was in summer. There was one of those drawn pictures on the cover of the *Wall Street Journal*. At any rate, that eventually got negotiated into a software licensing deal for a product we essentially didn't have. We would deliver it to them sometime in 1987 and they would incorporate this into their new product. That was a deal that I was actually able to get signed. I ended up signing it with a guy named Ed Belove, who later turned up at another company that I dealt with. Actually, the nature of that contract is what saved RSA. Basically we agreed to develop a product for them that would be a software toolkit. The people who were going to do the development were Rivest and another MIT professor, Shafrira Goldwasser. Then as it turned out, there was another MIT graduate that I hired in 1987 who also did a lot of the work. I ended up negotiating the deal with their attorney, and actually Iris dropped out of it somewhere along the way in 1986. They were interested, they liked the idea that we could help them, and they turned it over to Lotus to make some sort of a business arrangement. I went to this farmhouse where Iris Associates was located. This was where Ray Ozzie and a team of maybe half a dozen programmers were working furiously. We talked to them about what they were trying to do. They couldn't understand at first that this stuff could be patented, how you patent an idea. That's a recurring theme later on that appears in all of this. When I finally sat down with Lotus to negotiate the deal, they agreed to provide some prepaid royalties. There were two things that I got into that contract that really helped save RSA essentially. First of all, I remember saying, "When are you going to ship this product?". I'm trying to remember who it was from Lotus, I think it was Ed Belove that was responsible, he was VP of Engineering and Development for all of Lotus and this was all in his domain. He said, " Well, we're going to ship this thing in early 1987." I said, " OK. So what if you're late?" And he said, " Well, we're not going to be late." "Yes, but if you're late…" Also part of the deal was that they would give us some money, which was essentially prepayment against royalties we would collect for the sale of software that we were going to build and deliver to them. The idea was that if they owed us a hundred dollars one month in royalties for products they had shipped that used our software, instead of sending us a check for a hundred dollars, they would have prepaid royalties on credit. Their initial idea was that we would get nothing in advance, but that didn't make sense. I said, "Look, let's treat this prepayment as sort of a credit against which you can offset half of the royalties. So instead of sending us a hundred dollars they send fifty. They agreed to that. Then, knowing how long software projects can take, I said, "OK, What if you miss your date? What if you don’t make your date?” They said, “Well, that’s not going to happen.” I said, “OK but if you do I’m just trying to build a financial model that I can rely on here and a forecast I can count on. So if you don’t make it, how about you fatten this pool of prepaid royalties?” They didn’t like that but they eventually agreed to it because I had the better argument—which is that if they were right and were not late, what’s the big deal? And if they are late, “isn’t this appropriate?” This is one of those things where I think their attorney took Belove out of the room, or whoever I was talking with there. I think at one point they were actually thinking of just walking away from all this because it became painful, because I did this about three more times. I said, “ OK, what if you miss *that* date?” To make a long story short they missed them all. Needless to say it took them much, much longer than they thought. So every now and then these large checks would come in through 1987 and 1988 to provide just enough money to pay for office rent and salary and some other things. Along the way the next biggest thing that we did was in 1988 with what was then DEC or Digital Equipment. You know what I remember most about that meeting was going to sign the big deal in DEC’s famous farmhouse and Rivest showing up in his blue jeans and his flannel shirt like he wore everyday. I pointed out to him that this is probably a big deal and it might be appropriate to actually wear a tie today. So he said, “OK”. So he went back upstairs and he came back a minute later with a tie on, exactly the same clothes, but with a tie on over the top of it. So there was Lotus and DEC and then there was an end user software product. Rivest had some software he had been working on and it turned into a PC based software product that we never really sold very much of. However, it was a good demonstration tool and helped us to convince people that this stuff could work fast enough—something that everybody seemed worried about.

Yost: With the toolkit for Lotus Development, did export laws play into the whole thing?

Bidzos: Oh yes, of course.

Yost: Were the export laws an issue that was entirely for Lotus Development to figure out or did you get involved in that?

Bidzos: You know I don't think I realized until later—certainly at the earliest 1987, I think even later than that—what a big issue this was all going to be. I don't know if Lotus ran into some problems sooner than we did. I doubt it did, because I don't think they shipped that product until sometime early in 1990 or maybe 1991. I think it was early 1990, so I don't know how much discussion or how many problems or potential problems with the government they'd encountered prior to that. But some where along the way, in 1988 or 1989 I think it was, it became an issue for DEC. DEC wanted to build a multilevel secure operating system. According to them they had built one—a one level secure operating system that would incorporate a whole bunch of strong encryption. And they basically completely abandoned it, even after they had built it. Their stated reason for doing that was they were told in no uncertain terms by the US government that they simply wouldn't be able to market it broadly outside the US. They said, "Well that takes away too much of our potential market." Lotus, when they did start shipping the product in the early 1990s, it became a very big issue for them and they actually played quite a role in the…let's call it the battle with the government. I think it starts with the people who pioneered the field publishing their papers. Suddenly discovering that there is this large organization called the National Security Agency [NSA] that didn't like it. So there was sort of that phase. That was in the late seventies and early eighties. That firestorm got calmed down when Inman, who was the NSA director at the time, said something like, "Look, O.K., it won't all be classified. What we'll do is we'll have some sort of a committee to review papers [in cryptography, and cryptographic software—to classify certain knowledge on the premise of national security interests]. There will be both government and non-government people on the committee so you'll be represented." That quieted things down.

Yost: And that was all voluntary wasn't it, the NSA review process?

Bidzos: Oh yes. I think it was just a way for people to sort of step back, take a deep breath, or stop screaming at each other. So they did that for a while. Then in the late 1980s it got interesting again. The government introduced some sort of a program of its own. They had an idea to satisfy whatever commercial need for encryption there might be by just simply letting commercial customers become customers like government agencies were their customers. The State Department is their customer, the Defense Department is their customer. They sign up and enter into this complicated relationship of couriers sending keys around and proving you have secure facilities to put communication security equipment in, and that didn't work. Then it really picked up again in the nineties, and in particular when the government introduced something called the Clipper Chip. But along the way everybody tried to find some accommodation with the government for their product. As I recall Lotus didn't come out very well. Ray Ozzie came to the conference and spoke about this. I think that was probably 1994 or 1995 when he spoke about it. But at any rate their idea was to use a large key, but essentially give a significant portion of that key to the government. Nobody liked that because it just meant you were including the government. Not only are you making it possible for them to easily read everything that goes on, you're trusting them to maintain the integrity of their system of access. They did play a very big role that way. Ray Ozzie reached an accommodation that I think he decided was a good idea and nobody else agreed with, nobody in the industry outside of Lotus.

Yost: You mentioned the conference. Can you talk a bit about the origin of the RSA Data Security Conference, about both the founding and the early years of it?

Bidzos: Yes, actually it originated—you know there's another example where there's just one moment, one phone call where this happened—right about the time that the Electronic Frontier Foundation was being born around 1991. And actually it was also the time that something called CPSR, Computer Professionals for Social Responsibility, was becoming EPIC, the Electronic Privacy Information Center. The director of which is a guy named Marc Rotenberg. This was a time when the government made an announcement. I don't think it was the Clipper chip at the time, I think it was something called the DSA. Anyway they were starting to try to set or dictate [encryption] standards for the business community. They had made some announcement and Marc called me up and said, “They’ve just announced this. Have you seen this?” And I said, “Yes.” And he said, “What are we going to do about this?” And I said, “I don’t know. It sounds to me like the best thing we can do is educate people, so maybe what we ought to do is host a conference and educate people about this. I’ve got access to a lot of people who can talk about it.” It was his phone call, basically pleading, “What are we going to do? What are you going to do?” He was really bothered by DSA, seemed up in arms and didn’t know what to do. All that nervous energy that I felt somehow made me feel obligated to do something. So that’s when I came up with this idea to have this conference. So I got Rivest and a few other people, I think Marty Hellman was there, Taher El Gamal and some other people to say this is a bad idea and here’s why. And so we let people come for free, I think we got sixty people. It just seemed like a good thing to do again the following year.

Yost: What year was the original event held?

Bidzos: The first one was in the fall of 1991. I think the second one was in early 1993. And then it’s been January, February, or March every year since then. So that was the origin. With the conference in 1993, now the idea was, “OK, we need to educate people about RSA. We can leverage the brand name RSA a little further.” It was just a good marketing thing to do. So basically what happened during that time, between DEC in 1988…actually starting in 1990 and 1991, during those two years I signed contracts with Sun and Apple and Microsoft and Novell, and a couple other big players to provide all kinds of technology. In some cases it was just little bits and pieces of cryptographic technology. We got hired to do some code breaking for some companies that wanted to build compatible equipment, wanted to figure out what somebody's product did. At that point we had some customers, it seemed as if we were sort of like Switzerland, everybody would work with us and so it made sense to use this conference as a way to do all kinds of things: drive standards, organize some opposition to government policies, promote the RSA name, give all of our customers an opportunity. There's an ad campaign that some company does now, I can't remember who they are, but they say something like "We don't make the products you buy, we make the products you buy better." [BASF slogan, "At BASF, We…."]. So way back, I think there was a 1992 RSA security solution catalogue that would highlight products that other people made that had our technology in it, just to highlight it. So the conference was a good way to do that. It just grew steadily. It wasn't an overnight success. It's not something that succeeded beyond our wildest dreams, the idea was just to solidify our standing in the community, use the unique position we had accomplished in all these things. Not the least of which was to just simply make everybody understand and accept that RSA was the standard. That was the name of the game. In fact when the World Wide Web exploded in 1994 and 1995, when everybody who was building any kind of a product, people would come to me and say you've already done what we want to do. You're an Internet standard and you have the right, the same business model we have. They wanted help from us for all those things. It just steadily grew. Then we started adding an exhibitors' space and we always had people from the government who came, always gave them a podium from which they could argue their side. I think it was maybe the 1994 conference, I remember another one of those little moments... It was five thirty in the afternoon at the Hotel Sofitel in Redwood City and everybody had been sitting there pretty much since nine a.m. with a couple of coffee breaks and a lunch break. On the other side of the doors, outside of this large meeting room was a set up with bars and food and all this other kind of thing. I was moderating this panel of some government folks and some industry folks and we were really going at it. I looked out and I realized that we had gone thirty minutes over what we were suppose to and not one person had gotten up to leave. So I thought this panel and those of us on stage, this particular session is all that stands between these people and food and drink which they must desperately need and crave right now, it's late in the afternoon. They are all just frozen, stuck to their seats watching all of this go on. I remember realizing that we have some content that we're giving them that's unique, that we're able to put these panels together, bring people here, provoke people to say things they might not say somewhere else. There's some sort of talk show host aspect, sort of ring master kind of aspect, to it that I played. Some of these people I would just call and call until they would agreed to come. It was sort of a place to be, it was a place where everything happened. Then we started organizing separate tracks. It was a place where standards bodies could come and meet. It was a place where people started making investments in companies, started doing deals. And now, it has turned into this huge monstrous event where over ten thousand people show up and people like Bill Gates are eager to come because it's a place for them to make announcements about security. That's what it's become. It's become more successful and more important, just like computer security has become more important.

Yost: So even before the advent and growth of the Web in the early to mid-1990, RSA had really turned the corner as a business?

Bidzos: I think so. Yes, as you know there were a lot of network applications prior to this.

Yost: Of course.

Bidzos: There were many private networks in the early 1990s to the mid-1990s. The Internet I think was once reported to be growing at something like thirty percent per month. The only way that they were counting the number of people attached to the Internet, and the only way that could happen, is for these private networks en masse to start plugging in, start connecting. And that's what was happening. So there were those private corporate networks, which I understood very well. I understood what they were doing, what kind of products they were using. What I did was I went to the people who made those products. I ran around in the 1980s. Between 1986 and 1991 I must have run around and given hundreds of talks, talks to any group that would listen—groups within companies and groups at computer conferences. There weren't many at the time, and I started raising the issue of computer security. Yes, a lot of it was just marketing. I was trying to stimulate some demand. I was trying to get to these people to tell the people who made the products and tell them that they should incorporate security in their products. And then I would tell these people who made the products that they needed to do it with us because we had the best technology. In fact when I signed a deal with Microsoft in 1991, I actually ended up having to sell that deal three times. Nathan

Myhrvold was the guy I negotiated the deal with at the time. I made a couple of trips up and my attorney and I met with Gates and his attorney and it was a big deal even for Microsoft back then. I think that Bill Gates was barely worth a billion dollars at the time. Microsoft wasn't quite the company that it is now. It was a very small fraction in terms of its sales and volume. So even this amount of money was substantial for Microsoft. So finally it got to the point where we were going to conclude this deal where they would make extensive use of our technology in their products. Then at one point I got a call basically saying that "somebody called us from the government and said this would be a mistake don't do this or we're going to do something different, we're going to make a different standard and you're investing in the wrong technology." I had an idea who that person was so I called that person and basically just sort of screamed at them and said "this is illegal, you can't do this. You're either going to explain this to my attorneys or the *New York Times*, one way or another. You just can't do this. This is outrageous." After a few moments of silence, after I got done screaming the voice at the other end of the phone said I'll call them and apologize. And I said that would be really good. So that sort of blew over and then literally within forty-eight hours of that I get another call that says Bill's ready to sign this. But there's a rumor that somebody in Israel found a way to break RSA. So I email everybody I know and dig up everything I can on this and it turns out it is some academically interesting research, but that it has no bearing whatsoever. "I just got the right answer that says what you heard is wrong. Here's what's right." I think they came away from that even more impressed. I said this is part of what you get when you do business with us. What are you going to do when one of your large customers calls you up and asks you this question? You turn to us and we'll give you the same prompt service. We’ll get all the facts for you, help you assess it properly, and we’ll help you decide what to do. In fact, I pointed out to them that somebody had asked me “what if somebody broke RSA, your business would be dead.” I said “No, people would come back to us and ask us what to do next.” That was part of our business. So we put out that fire, then I get another call. This is exactly the time that Microsoft had hired a guy from Digital Equipment Corp. who was building a lot of what are Microsoft mainstream products now. Those were on the drawing board. His job was to get the next generation operating systems built and distributed computer systems built. He didn’t think that they needed any of this technology. He thought they could do it all with other more fundamental readily available technology. And so now I have to jump on a plane and fly out there and sit in a large room with him and a bunch of other people and essentially debate them all over again as to whether they needed this. At the end of a very long day I managed to convince them they should have it. It wasn’t easy, but yes, we had turned the corner so to speak. We were making enough money to where I think in 1991 I had maybe ten people that worked at the company, maybe not quite that many. It grew much quicker in the mid-1990s, which is when things obviously exploded. But yes, we had large customers. Apple was a very, very big customer. What we were doing for Apple, starting around 1990, turned out to be the basis for what VeriSign became.

Yost: Was the Microsoft deal the biggest deal that you had made to that point?

Bidzos: I think so. Novell was a pretty big deal too. Certainly in the networking business Novell was bigger than Microsoft. And Apple actually may have had double-digit market share back then, so that was probably a pretty interesting deal too. Actually I remember doing that deal. There was some point later when Jobs had started NeXT and we had a meeting with them about using our technology. And there were a lot of other smaller deals we had done, some special projects for a lot of companies. There was enough to keep us busy. We were making money we didn't have any debt. I was being very careful about spending money. I had to be.

TAPE 2 (SIDE A)

Bidzos (Cont): …I'm trying to eke out some sort of a business existence and make enough money. I was waiting for some of these people to get their products off the ground, which would then hopefully generate more income for us. Trying to fight these people to get these deals done was extremely difficult. They all objected for some reason. Their customers were not asking them for this kind of stuff. Even today people are reluctant to pay for security, back then they were very reluctant. So it was a very tough sell. Then on top of that, at the same time, I had to battle a lot of initiatives from the government that were actually designed to keep the market from ever getting off the ground. And then export controls, of course, we were fighting all of that. It was a tough fight and nobody else wanted to do it for good reason.

Yost: Cylink was in the hardware security area. Did you compete against them directly? And can you speak about how you came to form an agreement with them that later resulted in legal conflict between your company and theirs?

Bidzos: Yes. This is some more of the history that I discovered in the late 1980s. In the late 1980s I actually thought several times, “This isn’t fun. I should leave here and just go do something else. Because this market really isn’t going to grow for a while and it’s just too tough to do anything with this.” And then when all the sudden you start to discover that the government has a strong interest in this technology and there’s a lot more going on here than might first appear, that sort of distracted me enough and got me interested enough that I stopped thinking about doing something else. [Whitfield] Diffie told me most of what the issues with the government were, and he made me aware of what a big problem they could be. So that was sort of like telling me the secret that I think Rivest didn’t want to talk about too much because he thought maybe I’d get discouraged or something like that, or maybe just thought it would be a distraction. So after that I would say this business with MIT and Stanford and the dispute over who invented what, and the patents, was sort of the other thing that I never quite understood that all of the sudden I realized. I had a couple of interesting phone calls. One was from Cylink, and another one was from Newscorp. Adi Shamir was forming a company called News Data Com, which would be an arm of Newscorp that would build secure smart cards for the sky TV system in Europe. There’s some Australian guy who ran all this for Rupert Murdock and he called me. Well I got a phone call from him one day in late 1988 basically saying “I work for Rupert Murdock” in a heavy Australian accent, “ and I want to buy fifty or a hundred percent of your company.” Well, I guess I’ve taken the call, I might as well try to respond. I said, “Oh, Ok.” So I made a few trips to London and we had some negotiations, we just couldn’t come to terms. I just didn’t want to sell out for what seemed to me nothing, which is what they wanted. Another phone call I got was from Cylink, from Lew Morris, or maybe it was from Jim O'Mura. It was either from Jim O'Mura or Lew Morris, I don't remember which one it was. They basically said, "We've got this problem." So this is when I started to learn the history of the Stanford claim that they invented all of this [Diffie and Hellman] and that RSA was just a logical and obvious extension. But since the patent office didn't buy that I think the claim was that they had the Hellman-Merkle patent, which was a patent around the "Knapsack System," the public key cryptosystem based on the mathematical problem of knapsacks. They claimed this was more broadly the invention of public key encryption. Well, what we believe, what I believe, what my lawyers believe, all sort of became irrelevant. We thought, "Well look, it might be better to just pool the patents and form a partnership and try to make the universities and all these inventors and ourselves and the broad community in the market place…not not happy in some cases and happily oblivious in other cases, so they don't have to deal with this problem." So we did, we formed a partnership to hold the patents and we would retain all the rights to go off and do whatever we did. Cylink made hardware and we made software. That worked for a while.

Yost: So the Hellman-Merkle patent was held by Stanford University, just like the Diffie-Hellman patent?

Bidzos: Yes, there were three patents that Stanford had. One was the Hellman-Merkle patent, which was knapsacks as sort of the preferred embodiment, even though they'd been broken. Then there was the Diffie-Hellman patent and then there was the Hellman-

Pohlig patent. Those were the three patents that Stanford had. And we had the RSA patent.

Yost: And Cylink had purchased a license for the patents that Stanford held?

Bidzos: Cylink had a relationship with Stanford that was something like our relationship with MIT, although I think it was different in some important ways. Just one thing I didn't mention is that in 1990, maybe April of 1990—I seem to remember just trying to visualize the date on the letter—I made a deal with MIT where in return for some equity in the company they granted us exclusive rights to the RSA patent for the rest of its period of validity, its term. If I hadn't done that it would have become automatically nonexclusive about a year later.

Yost: Was it a hundred and fifty thousand that was paid to MIT by Rivest, Adleman, and Shamir to acquire commercial rights to the patent?

Bidzos: Yes, that was the money from Dr. Kelly. I think Kelly put up something like two hundred thousand, which was mostly used to get MIT the money for the patent. And this New York group also invested. I remember the name of their investment banking company, but it doesn't matter, because it changed about eight times.

Yost: But MIT still had some claim after…

Bidzos: No. MIT got a hundred and fifty thousand dollars. And what RSA got was the exclusive rights to the patent up until some point, a fixed date in time at which point it would become a nonexclusive. So RSA could keep doing what it was doing, but so could everybody else. So it was about that time that the patent was about to become nonexclusive and I thought, “Hey we don’t want to do this. This is a very difficult business, we’ve invested a lot in it. We’d like to continue this and we want you to go along with us. So take some equity in the company.” By the way, to fast forward a bit, at the time, I think there might have been one or two that sort of changed what I’m about to tell you subsequently, but at the time, in 1997, I think the MIT patent had brought more to MIT than any other invention that came out of the school, including core memory and penicillin. And it was by virtue of this deal that we made that, they got equity in the company and so it was one of the early times they did that. Our relationship with MIT was pretty straightforward. At first we had bought patent rights exclusive for a period of time, then nonexclusive, then we renegotiated that in return for equity in the company, it became exclusive until the patent expired. Now Cylink’s relationship with Stanford was similar, but I don’t know all of the details. Cylink got to practice whatever the patents described and then they would also have the right to license those patents to other people. And so we pooled all of those patents in 1989 I think it was shortly after there was a big earthquake out here. I think that was in October of 1989. The earthquake disrupted the World Series out here so it was in the fall. I’m not really much of a sports fan, but it was in October. I was in Boston when it happened, which is when I got this call. What I remember is coming back and beginning the long process of negotiation with Cylink that ultimately culminated in the formation of this partnership, Public Key Partners (PKP) as it was called.

Yost: What specifically led to the problems within Public Key Partners and with Cylink?

Bidzos: I haven't thought about some of this in a while, but the basic problem was this, we had some sort of an argument that we already had from Stanford through MIT all necessary rights to the Stanford patents to do whatever we do with the RSA algorithm. I think there was a very legitimate claim, a very defensible claim that when we got this from MIT, it came with both, that MIT and Stanford had some relationship and through that relationship there seemed to flow some rights that came to us. I think Cylink claimed that they didn't and we claimed that they did. But it kind of became mute because we put that issue aside. We stopped arguing about it. We continued to claim that we had them and we just dropped our dispute about whether or not RSA already had from Stanford via MIT any necessary rights to the Stanford patents, which means that we can stop arguing about whether we need to get any because we think we have them. Aside from whether we think we need them, we already have them anyway. But Cylink clearly had no rights whatsoever to the RSA patent. And when we formed a partnership there was language in the partnership that said if Cylink wants to practice the RSA method they can come to Public Key Partners and get a license to do that. I think at the time Cylink was building hardware that basically had used the Diffie-Hellman algorithm. Now this is something I found out later. Apparently they had a very large customer, an international customer that absolutely insisted on the use of the RSA algorithm. And so I found out later that Cylink in fact had built this product and then said, “Oh gee, we need to get a license to do this.” And so they started approaching us for a license and they started making some really outrageous demands for a much broader license that essentially would give them all the same rights that we had, which was unacceptable to us. And again I only found out later that at this time they had already shipped products. My opinion is that they overreached when they said, “We want a license.” In fact I remember having a conversation with them where I said, “Look, if you want to start with a simple license, very low royalty, very reasonable best terms we’ve ever given to anybody else, you guys can have it. Obviously you deserve that or even better—to go make your hardware, we’ll give you that. They wanted more, which basically triggered a whole bunch of lawsuits.

Yost: At one point, I understand the government offered to pay PKP a royalty fee in using DSA but backed out of that and you acquired the Claus Schnorr patent.

Bidzos: Yes, a little more complicated than that but the simplest way to describe it would be this. The government said we want the DSA to be the standard and this German fellow named Claus Schnorr claimed to have a patent that covered the use of the DSA. It turns out that a couple of the folks from the government had gone to Germany and talked to him. He told them he wanted a couple million dollars for the rights to use his patent. They apparently were reluctant to pay that. They balked at paying anybody that much money. So I went over there to see the good doctor and had a long, long lunch with him. Basically by the time I got done with him, he basically signed over the exclusive rights to his patent for nothing except the promise of future royalties. And I think it was because he concluded that we knew how to build a business around this technology and I would be the best person to represent his patent interests. I think it’s like a sports figure wanting somebody to go negotiate his contract for him. He did not want to negotiate it himself.

Yost: And in the end it worked out for him?

Bidzos: It worked extremely well for him in the end. But the interesting thing that played out is that I showed up in a meeting with some government folks and in very bad German with an English accent….They basically said are you going to let us just give you a little bit of money for any rights to the Stanford patents that might cover what we’re doing so we can get on with our DSA. And I said something like “You’re infringing my patent, my German patent.” So they were not happy about that. So basically we agreed to make a deal where they would say we have the DSA and it’s covered by the way…to the extent it might be covered by these patents and it would list the Stanford patent and the Schnorr patent—then you need to go get a license. We’ve negotiated the terms of a broad uniform nondiscriminatory license that looks like this. And I negotiated this deal with these government folks and I think that this would have produced a windfall for Public Key Partners that would have been amazing. I think it would have cost—anybody who wanted a license had to pay $25,000 to execute the license and then they would have had to pay 2% of the value of the products they sold, with a minimum. So as people set out building products we would have made a lot of money. Some of the people from Cylink wanted, instead of charging royalties, they wanted to charge a dollar per certificate—envisioning that there would be lots of certificates down the road, not understanding the business and not understanding reality. They didn’t understand that that would be unacceptable to a lot of people for many, many, many reasons. So basically Cylink insisted that we make that demand. I visited Cylink a dozen times during this period arguing for hours with some of their people that this was a bad idea, that it won’t work, it’ll be unacceptable. We’re going to kill this potential golden-egg-laying-goose here. If as you guys say you really believe that this is the moment—that this is what the universities and the inventors and us, the people who’ve developed the market and done all this, if this is the culmination of our efforts then—and it is, and it’s big and you’re about to kill it. You don’t want to do this. They absolutely insisted so that became the position we took. By the way the government was ready to go with the proposal I negotiated with them. So at any rate, it all suddenly fell apart. Everything stopped. And it turned out, as we found out later, a few European governments and the Canadian government had specifically written in and said this requirement to pay you for certificates is unacceptable and we simply won’t do it and we will not support this anywhere, ever, period, thank you, end of story. So greed really killed in this particular case.

Yost: You mentioned key escrow in the government earlier. Can you talk about your response to Clipper and the role you played as a spokesperson against it?

Bidzos: Yes, I was a gadfly I guess, and sort of an organizer of the opposition so to speak. Here’s another case where the conference became a great place for this subject to be discussed. It was a venue for people to state their concerns, including civil libertarians and people in the industry who where going to be effected. I think there was just some sort of organization needed to do all this and the conference proved to be the perfect place. To the extent that I emerged as any kind of a point man or a spokesperson it's because I had the microphone at the conference and I understood all the issues and I knew all the people. They were happy for me to represent some of their concerns. We became the tip of the spear, so to speak, in this fight against government efforts to do this. But I think it was broad industry support obviously that made it all happen. In 2000 the government finally backed off of export control. Key escrow just turned out to be a bad idea. It was just obvious that key escrow doesn't work. Sometimes I get blamed by government people for having unfairly caused people to reject some of their proposals. I think there are some people who still think that I was all that stood between them and a market full of key escrow products where they could spy on all the bad people they wanted. It's so naïve. First of all, if I had that much power and influence it would have been something. But secondly, it just wouldn't have worked out that way. Nobody liked it. I think that's what they never saw. It was so clear to me, I could see it so easily, that nobody liked it. In fact I think I did a couple of things. One is I met with some government folks…I just said, "Look, I've spent a lot of time thinking about what I would do if I were you. Here's what I would do. If you're interested." And they seemed interested. They sent a few people out, some of whom I never got a name or card, never met again, sat in the back of the room or in the front of the room. They never said a word, maybe asked one or two questions. But basically I just mapped out a…first of all businesses want key escrow they absolutely have to have it. It's a liability issue, it's…you name it. It's good corporate governance it's everything else you can imagine. And individuals don't want it. Here's some nice ways to encourage the development of key escrow products. Here’s a way to structure everything so that you encourage it without making anybody angry, without telling anybody that they cannot have the privacy they want. You can minimize this problem tremendously with this approach. A lot of good thinking went into that. I think they appreciated that and they took it away and took back some ideas. But they just couldn’t move that quickly and there are other people who make decisions who weren’t in the room. And that’s that. But eventually they gave up on all this stuff.

Yost: Did the development of the World Wide Web, and the initiation of new firms, such as Netscape, did this come as a surprise to you or did you long see that this was the direction of networking and the way the Internet was headed? Was your perception of what networking would, or might, become a factor in your staying with RSA over the long haul, seeing great long-term opportunities?

Bidzos: Yes. Well, I had no idea that putting a friendly face on the Internet was going to make it explode the way it did. But I did have a good idea that pretty much what’s happening now was in our future. I mean it just made too much sense, it’s too convenient, you could see people becoming incredibly more efficient by making full use of it. You could see cyber society coming. How it was coming and how fast it was coming, I don’t know of anybody who accurately predicted that, who could say somewhere in the mid-nineties something will happen. But you know I was in a position of having a very, very nice view into what was going on and I talked to a lot of people about it all the time. That was my job that was what I did. So I don’t think I saw anything that anybody else wouldn’t have seen, being where I was and talking to people that I talked to. What I might give myself credit for in terms of anticipating the future was at least having a very strong belief that it would happen and it would happen soon enough that it was beneficial for me, that it was in my interests and the interests of RSA’s inventors and shareholders and the universities and everybody who had a stake in this for me to build the company as if that was going to happen very soon. And the proof is if you look at the deals that I cut in 1990, 1991, 1992, and 1993. There are probably about a hundred business agreements that I negotiated during that time frame. And what you learn from looking at how they are worded…if I were looking objectively at this now I would describe it as saying, “Oh, whoever wrote this thought something big was going to happen, didn’t know what it was, basically they drew a line that said anything beyond what we can see right now, you have to come back and talk to us again because there is going to be a very different world.” And so that is part of what made negotiating all this difficult. Microsoft always sends a low level guy who’ll come out and says he’ll make you famous and give you fifty thousand dollars while Microsoft takes your technology and uses it. That was very nice and after he came down about three times is when one day Gates finally showed up and we started getting serious about it, but even then he honestly said things like “nobody’s asking us for this. I mean we have to anticipate, it is very difficult to justify the investment. We have to have the freedom to do these things with it and this that and the other.” The hard part for me was to avoid saying, “Yes, I guess you’re right.” I had to say, “OK, that’s fine but what if *this* happens.” One of these people…actually this argument was very effective because he’s so smart. You can say, “OK. Well, what if this happens.” And he’d go, “Yes, O.K. you got me there, well I guess we shouldn’t do that.” “And what if it plays out this way. I lose and you’re telling me your intention isn’t for me to lose, but here’s a scenario in which I lose.” So after three or four of these then you get him to agree to just sort of block off the future. If things don’t change much and your market grows based on the products and the usage and the value of the technology the way we understand it now, that’s great you shouldn’t have to pay me much more money, if any. But if all these other things happen as I’m telling you I think they will and if I’m right don’t you think I deserve to get more? And they would say yes. And so you see all these contracts have all the same restrictions, very strict restrictions built in. The other thing that I did is, starting about that time in the early nineties, as early as 1991, basically started obligating people to incorporate my root public key into their products. Again, I could see what it would take, what kind of an infrastructure it would take for this technology to work on a grand scale. And so I started seeding the market that way. As early as 1989 I had laid out that we’re going to need a separate company to do this. We can’t have this under the same roof. This is a different business and so I started laying the groundwork for what became VeriSign way back then. In fact, when VeriSign was formed in early 1995, by then there were many, many millions of products that already had VeriSign’s root key in them, actually before the company was even formed. And all the RSA software was built and licensed and incorporated into all these products, with that key compiled in and built in and ready to be used. And the benefit of the RSA name that already had been accepted as the standard …you don’t have to explain to anybody why your encryption is any good or what this whole public key business is about. RSA had spent at that point ten years doing that already. And I would tell people in the early 1990s that there will be a company that does this and the way I described it was that if you look at the skyline of technology companies in the year 2000, probably Microsoft and IBM will still be in there, some we haven't heard of will emerge, but this digital certificate company will be one of these new companies. I tried in 1994. In March of 1994 I got a whole bunch of big companies, including IBM and GTE and others together, and said, "Let's form this company. I'll form it. "I want you all to be partners." So finally I tried and everybody was too busy, in 1994 the Web was exploding. And then in 1995 it finally came together and Visa, Intel, Ameritech were the founding partners in all of this. They understood. The infrastructure had been built, and the groundwork had already been laid. It was going to happen.

Yost: So spinning it off as a new company, VeraSign, was to bring in these big partners?

Bidzos: Oh yes, the reasons for doing it were many. I mean one of them was that RSA was closely held. There were just a few of us that owned most of RSA. It didn't make sense to try to explain to people, let people invest in RSA because of this, so that was one reason. But the other reasons…The top reasons went something like this. One is to make it easier to finance, second is to be able to bring in the partners that would be necessary to make it succeed, because Microsoft's customers aren't going to trust IBM to sell their certificates and neither are IBM's customers going to trust Microsoft in general. In fact IBM will keep Microsoft from selling certificates to its customers. So my pitch was we need to all do this together. And the other thing was that I thought the value of RSA was its laser like focus on doing encryption. We do one thing and we do it better than anybody else. We did a lot of really good things…in some cases things really good for the community and also clever and good for us. The conference was one, the factoring challenge was another one. Helping people understand why our technology is good, getting out in front of everything. I thought that the value of RSA would be diluted. “You know, RSA does encryption. Yes we’ll do this service thing too with certificates. I mean, yes, we know how to do both of these things, don’t worry.” There were a lot of people, some of them who worked around Jobs, some of them who worked around Gates, who understood that by say 1992 or so I think they were starting to say, “Ah look what this guy’s doing. This is going to be interesting.” And they were already saying, “We’re going to build this public key in but we’re never going to trust you to do this for our customers.” I said, “OK well don’t worry. Somebody else will do that.” So there was this certainty on my part that we would just end up fighting too many battles trying to convince people they should trust us to do all this. It just wouldn’t work. I wouldn’t trust a company to do all that. So there were a lot of reasons to spin it off separately. And also to just let it grow and pursue the market the way I wanted to. That I will say worked out very much according to plan. And then of course, through a whole bunch of acquisitions and other growth strategies it has done things beyond the original charter, but it still makes hundreds of millions of dollars a year in high margin revenue from selling commerce certificates, and it still dominates with eighty to ninety percent of the market. That worked out pretty well.

Yost: Yes, it sure did. You continue to serve on the board of VeriSign don’t you? Are you still chair or is it vice-chair? How actively are you involved these days?

Bidzos: I'm vice chairman now. I was chairman up until I think a couple of years ago. We signed some big contract with the government that required that people who held certain titles get security clearances. I wasn't going to be one of those people. But yes, I'm not very involved. I am at the corporate governance level, I'm on some committees. But in terms of the day-to-day business, I'm not that involved. And I left RSA's board maybe three years ago, something like that. It's kind of interesting now that RSA and VeriSign actually started competing quite directly. It is a really kind of an interesting sort of thing. VeriSign has started selling tokens that compete with RSA's that use certificates and leverage VeriSign's infrastructure and it is just sort of funny how it's all evolved. But to answer your original question, yes I believed. I was going to great pains and spending a huge amount of time and energy and going through great frustration in order to negotiate contracts that anticipated what was coming. And if it was going to be more than five years away then this would have all been sort of forgotten. So I believed it was going to happen. I was always optimistic. It turns out that looking back, historically, a lot of things you hear are true. People would say it takes a generation to really exploit new technology. That's true with public key, almost two generations. It's thirty years now. But if you look at the public key infrastructure that was built by Netscape and later by Microsoft, that happened pretty quickly.

Yost: Was there a concern at the time of forming VeriSign of competitors in this area, specifically the Postal Service, but others as well?

Bidzos: Oh yes, they were in there. Oh my god, you name it everybody thought they wanted to do this. Everyone of the…GTE did it. They formed a division that did this. Everybody outside the United States was going to do it because they weren't going to let us do it. Oh yes, everybody thought they were going to do it, but I had the inside track. I had the software of public key already out there. I think maybe more valuable than all that even was the name RSA. I had spent ten years and a lot of time and a lot of money promoting the name, establishing it, getting it trusted, getting people to understand that you don't want to try to do this stuff, you don't want to mess around, it's better to leave it to somebody who specializes. That really helped as much as anything else. But yes a lot of people tried to do it, wanted to do it, are still doing it but we still have ninety percent of the market today. The Postal Service is a great example. They just thought that…I think there are probably a dozen government agencies that thought they were the right ones to do this.

Yost: That basically covers the major areas I identified and wanted to ask in this interview. Are there important areas I've missed or are there other things that you'd like to add?

Bidzos: No, not really. I haven't thought about some of this stuff in a few years. I am kind of retired. My last full time operational position was with RSA ending about four or five years ago. Although I still stayed on as conference chairman, but I even retired as conference chairman last year. It is interesting thinking about the questions you've asked. I think those are pretty much the highlights as I remember them too. I mean there's this interesting academic development. As we talked about [just prior to the interview] I think there are some people who haven't gotten proper credit for what they did, people like Ralph Merkle and Steve Pohlig. And a student at MIT whose name escapes me, the MIT student who did the paper...it just sort of alerted people to the idea that you could apply this to public key. And then there are a lot of people in the business world I think who never quite got all the credit they deserved. Bart O'Brien would probably be one of those. He had tremendous enthusiasm. I think he had a pretty good idea that this would become important. I know he gave me a book called *Security for Computer Networks*. It was written by a couple of scientists, one of them a British guy who I met later. But there's just a page in there where he states you can do all kinds of really cool stuff with this, in so many words, something like that. Bart showed me that and said I think this guys right. He said "This going to be really exciting." A lot of people say, "Oh what a great vision of all this you had." And I laugh and say, "The people who wrote about this stuff in the 1970s…it is just a question of whether you believe what they said or not. Rivest, Shamir, and Adleman, and Diffie and Hellman and Merkle, those guys had a great vision. These people really had the vision. The problem is that…they knew all this would happen, but they didn't know when. And when they set out to start a business and spent money and took other peoples money to spend…then *when* that become the only important question. I think that's the credit I would willingly take for my contribution would be to sort of bridge that gap between this is going to happen and it happening, of buying into the vision and building it in a way, understanding it in a way…The proof that I understood their vision and maybe even thought about it in business ways was the way I built the business over those years, because it clearly anticipated all of this in some very specific ways. And so that turned out to make the companies very, very successful and lots of people had a lot of good financial success. But I think if you ask Rivest, Shamir, and Adleman, I think that they're sort of happier seeing…they're really excited about the conference they love coming to the conference. They love seeing the companies name on lots of products. I think that means even more to them. I'm sure if you ask MIT they're happy about the money. I never complained about the money, but if I was doing this for the money I probably would have left and would have done something else in the 1980s. This was more interesting and more fun than anything else I'd ever done.

Yost: And of course Rivest, Shamir, and Adleman were honored with the Turing award recently.

Bidzos: Oh yes, of course. They've gotten good recognition for their work, but I think they like the recognition they get outside the academic world as well. All that stuff is important to them and I think they've come to terms with Marty Hellman and some of this whole business about the Stanford patents. There's some really interesting…that's sort of an interesting story all on its own. There's that sort of Hellman-Pohlig work that was right on the verge, but it wasn't there yet. It wasn't. It turned out to be a symmetric cryptosystem that has the structure of RSA but none of the properties. But clearly it was on the way. And I can understand the frustration of being a real pioneer. I think Hellman many times doesn't get the credit that he deserves. I mean I think you'd have to call him the father of all of this in a sense, he and Diffie of course. But Hellman brought Diffie and Merkle in. And Pohlig, he's just really an important guy as well. Some of the other ones some of the other folks... I'm just drawing a blank on some of these people. But there's a guy who used to be on the faculty at Berkeley who is now I think at Carnegie-Mellon—Manny Blum. So there are a lot of interesting folks who all played some role in all of this who didn't make any money, didn't get any of the fortune or the glory. And it's just kind of unfortunate. Their stories have never quite been told and they've never really been recognized for what they did. Except maybe in that room where we all had dinner a little while ago and talked about all of this.

Yost: Thank you so much. It's been fascinating and very helpful to record some of these important historic developments, and the contexts of these developments. I really appreciate you taking the time this morning.

Bidzos: Sure. No problem. You made it very easy for me. I appreciate that. No pictures that's always good.