Ralph Merkle:
2011 Fellows Interview

Public-Key cryptography

Interviewed by:
Jon Plutte

Recorded: March 11, 2011
Mountain View, California

CHM Reference number: X6074.2011

<crew talk>

Plutte: It's March 11, 2011, and we are interviewing Dr. Ralph Merkle at the Computer History Museum. Thank you very much for joining us. I'm going to ask you a series of questions about the basis for Fellows Award. If you can give us a fairly quick and concise answer, that would be great. What is cryptography?

Merkle: Cryptography is sending secret messages so that even if some enemy intercepts the message they can't figure out what it is. All they see are meaningless scrambled letters.

Plutte: What is public key cryptography?

Merkle: Public key cryptography lets me send a message in secret code to someone I've never met without having arranged a secret code in advance.

Plutte: How does that work?

Merkle: Public key cryptography works by my sending you my public key, and also sending my public key to *everyone,* including any eavesdroppers, and then having you encrypt your secret message to me using my public key. I'm the only person in the world who can decrypt the secret message because I'm the only person who knows how to decrypt messages encrypted with my public key.

Plutte: Why is that important?

Merkle: It used to be in order for me to send you a secret message we had to first arrange for a secret key, and the way we arranged that secret key was for me to create a secret key and send it to you by a courier: the guy who had a briefcase chained to his wrist and would drive over on a motorcycle and hand you the key from the briefcase. That was a big problem. A lot of times we hadn’t made that arrangement or it was expensive or inconvenient. The reason public key cryptography is important is that it eliminates the courier. You can set up your keys on the fly when you need them without advance preparations.

<crew talk>

Plutte: Please do that again. That was a great description.

Merkle: Okay. The big advantage of public key cryptography is that it eliminates the couriers. In conventional cryptography, if I want to send you a secret message before we can do that I have to create a secret key, put it in a locked briefcase, chain it to the wrist of a courier, and have the courier drive off on a motorcycle to you. You have to open the briefcase, get out the secret key and then *after* we've done that *then* I can start sending you secret messages.

<crew talk>

Plutte: When did you first think of the idea of public key cryptography?

Merkle: I first thought of the idea of public key cryptography when I was trying to think of a quarter project in 1974 when I was taking a security course at Berkeley. I was trying to figure out how to reestablish security between a terminal and a computer system after the security had been compromised and the enemy knew every detail of what was going on. And the question was: how do you reestablish secure communications when the enemy knew everything? That's the basic problem of public key cryptography. If the opponent knows everything, how do you establish secure communications over an open communications line when the enemy is listening in?

Plutte: I read that you developed a scheme called Merkle's Puzzles. Can you talk about that?

Merkle: When I was thinking about how to establish security for the project for this course I was taking I thought about the idea of puzzles, which are now known as Merkle's Puzzles. The idea was simple. Let’s say I want to communicate with you. I could create a whole bunch of puzzles and send them to you, and you could then just throw away all of these puzzles except one, which you'd pick at random, and you'd crack just that one puzzle. Now it takes a fair amount of work to crack even one puzzle but when you cracked it, inside the puzzle you find a number, “I'm puzzle #437”, and you find a key. The key is some random string of bits. You send the number back to me. You say, "Hey, I solved puzzle 437". So now I know the puzzle you solved because you told me over the open communications channel, and that means something to me because I have a list of all of the puzzles indexed by their puzzle number, but it doesn't mean anything to the person who's listening in because the puzzle number is inside the puzzle. Until you crack the puzzle, you don't know what the puzzle number means so the eavesdropper hasn't learned a thing except somewhere in this pile of puzzles there is a puzzle #437, but to find out which puzzle is puzzle #437 the eavesdropper has to solve all the puzzles.

Well, if I've sent you a million puzzles the eavesdropper’s going to have to solve a lot of puzzles to find out which one you cracked, and you only cracked one so it didn't take you much work, and I created the puzzles, which I can do quickly and easily so it didn't take me much work, and that's Merkle's Puzzles. It's a fairly simple idea but one that provides you with the basic concept that I put in a small amount of work, you put in a small amount of work, but the eavesdropper has to put in a lot of work.

Plutte: As you were working on this project, and I know it was for a class, did you have a moment when you went "Oh, that's it."?

Merkle: When I thought about how can you possibly establish security when everything is known to the eavesdropper, and the eavesdropper can listen in on communications, how can you possibly establish security? So my first thought was: it doesn't look like you can, so I'll try and prove that it's impossible. So I tried to prove that you couldn't establish security, and I tried and I tried and I tried and I failed miserably. Then I thought about it some more and I said, "Well, if I can't prove that you can't do it I'll turn around and try and figure out a method to do it." And when I tried to come up with a method for doing it, having just tried to prove you can't do it, I knew where the cracks in my proof were, so to speak, and I knew where I could try and slide through. So I worked on those places and lo and behold it turned out it was possible. I could use the cracks in my proof to come up with a method for actually doing it, and when I figured out how to do it there was this, well, the traditional "aha moment" where I said, "Oh, yeah, that works. I can do it." That happened very rapidly. It was all one night of staying up late and thinking and then realizing “Oh, my gosh, I can do this thing. It seems very counterintuitive but I can actually figure out a key. I can establish a cryptographic key over an open communications line even if the enemy, the interloper, the eavesdropper knows everything”.

Plutte: That's great. What year was that?

Merkle: Fall of 1974 when I was an undergraduate at UC Berkeley taking CS244, which was a computer security course. My great ambition at the time was: “Can I develop a quarter project?” It turned out the idea was worth somewhat more than a quarter project but at the time that was what I was trying to do.

Plutte: That's interesting. The development of this obviously is being applied now to web browsers and all the internet but back then there was very little internetworking. Did you ever foresee that it would be used for transactions and for all the things it's come to be used for?

Merkle: When I first thought of this idea my first thought was oh, this is going to be very useful for sending secret messages over communications lines. It looked like sort of the traditional thing they used in various sorts of cloak and dagger activities, but at the time there was not a lot of usage of the web, certainly nowhere near as much usage as exists today. And while it did seem as though it would be useful the current huge amount of usage was not something that I envisioned at that point in time.

Plutte: Just about this same time a couple of other folks were working on a very similar idea. How did you connect with the other two fellows?

Merkle: Well, there was a person in the class that I was taking, CS244, and he was also interested in cryptography, and as it turned out he was in touch with Whitfield Diffie and Martin Hellman who were at Stanford. I showed him the drafts of the work that I had done and explained the ideas and we talked about it very animatedly, and at some point he was in touch with them and one day when I was talking with him he said, "There are these guys at Stanford who talk just like you." And that was the clue that there was someone else in the world who actually was interested in these kind of ideas. I tried to get in touch with them and finally succeeded. Once we found each other we realized we were working on similar projects and similar ideas and got together. At that point in timeno one thought this was possible. When I talked with people they sort of looked at me in this very odd way, which said “What are you talking about? What do you mean communicate secretly over an open communications line? That doesn't make any sense. How can you do that? You're talking crazy talk here."

Plutte: You got in touch with the guys. What was the process of you actually working together?

Merkle: I went up to Stanford for a summer and we started working on developing some actual systems that would be efficient and useful. The puzzles method which I developed was obviously a demonstration that you could have a method where if you and I were communicating we could force an eavesdropper to put in more work than we put in, but to have a method that was really of interest you wanted to have a method where the person who was trying to eavesdrop had to put in a whole lot more work. In fact, you wanted the eavesdropper to put in an amount of work that was preferably exponential in the amount of work that the two people put in in order to establish the cryptographic key, and of course that was something that we wanted to achieve and we developed some cryptographic techniques that would hopefully let us do that.

Plutte: Martin Hellman talked about the interest and resistance from the NSA and the CIA. Did you experience any of that and what was your experience if you did?

Merkle: We did a lot of work and obviously there was a great deal of interest in a wider community. There was a lot of interest on the part of the defense and on the part of the government in our research work. I never had a lot of direct contact at that time with the people who were in the government and in what their interests were and what was going on so I don't have a lot of direct knowledge of what the political ramifications were. Mostly I got it indirectly. There was a lot of discussion. For example, when I was going to give a talk, along with Steve Pohlig, another graduate student, at one of the conferences, we received a letter that was suggesting that giving a talk at an international conference would constitute export. There was a flurry of activity among various lawyers at Stanford and discussions with Martin Hellman. After a great deal of discussion about what the possible legal issues were and who could be defended and so forth and so on, the conclusion was that Hellman, because he had a tenured faculty position at Stanford, would be easier to defend legally in case there was some legal problem. So he actually presented the paper which we were scheduled to give at the conference. That's about the only

case where it actually had a direct impact on the work I was pursuing or had a direct impact on me personally.

Plutte: As you did this work, what was the most challenging problem you faced?

Merkle: Cryptography is a very complex field. you are trying to create problems that are difficult to analyze but which nonetheless can be solved if you have the correct information. We don't yet have the theoretical apparatus which lets us prove that the problem that we think is hard, namely cracking the cryptographic system, is in fact hard. So you have to rely on your own intuition, which is notoriously bad in cryptographic systems. There are many, many, many inventors of cryptographic systems who come forth and say, "I have invented the unbreakable code" and of course it's broken, so in cryptography what we rely on is not the individual inventor of the cryptographic system; what we rely on is a larger community. An inventor will come forward with a cryptographic system that they think is good. Then they will publish it and ask others to try and break it. Then others will try their hand at breaking the system, and if many, many, many people try and fail to break a cryptographic system, then after years of such effort the cryptographic community as a whole will say, "Well, we think - because so many very bright people have tried and failed, we think the system looks like it's reasonably secure". This is not a theoretically sound basis but it provides some degree of comfort. This is how we develop cryptographic systems. This is how, so far, we decide that cryptographic systems are good cryptographic systems. We are beginning to have some ability to say a few things theoretically about cryptographic systems, but it's still in the early stages, and as a consequence the really hard thing about cryptography is not inventing cryptographic systems, although that is a challenge. The really hard thing in cryptography is establishing that a cryptographic system actually is secure. So the few systems that are well established and that have been extensively studied are very valuable not because the inventor invented them, although they get a great deal of honor because their system was chosen and was judged worthy of the extended study that goes into them; they are valuable because of the extended study by this large community and because they have withstood extended study and attack. And they are valuable because now that we have studied them so extensively we now feel we can rely on them. The handful of systems that have been extensively studied are really quite valuable.

Plutte: Great.

Merkle: Which is too long for a sound bite but--

Plutte: It's a great description. Maybe here's one that we can go a little shorter on. The technology developed enables billions of dollars in safe commerce on the internet yet in an interview of Martin Hellman in our interview today basically said that you've made almost no money off this project. Why not and are the intrinsic benefits of creating it enough?

Merkle: One of the very interesting problems that we as a society face is how to provide incentives to people to create valuable and worthwhile innovations, and I have to say I think as a society we're not very good at that process; we're not doing a good job at providing effective incentives for providing truly new and truly creative concepts or ideas and rewarding them. There are various reasons for this. To a large extent, we reward incremental improvements and we reward evolutionary improvements and we do this for many reasons. One, we can understand incremental improvements and stepwise improvements more easily than we can understand large improvements or revolutionary improvements, and it's easier to recognize and reward small steps or incremental improvements. When it comes to major improvements we really have a very hard time understanding them. It's many years before they work their way into society, before society really begins to understand them, and as a consequence we don't provide the kind of incentives and the kind of rewards that we do for the smaller, the more incremental improvements.

<crew talk>

Plutte: It's enabled billions of dollars in saved commerce. You are answering that, but I wonder if we could do it in a shorter way.

Merkle: Briefer.

Plutte: Yeah, something briefer.

Merkle: So what's the brief, succinct answer.

Plutte: Yeah.

<crew talk>

Merkle: One of the interesting things that emerges from all of this is a question which is at the very core of society as a whole: how do you reward really novel ideas? How do you provide incentives to people for providing really major innovations? Right now, we don't do a very good job. If you produce a small, or incremental or evolutionary advance, there are clear mechanisms that provide pretty good rewards and pretty good incentives. If you provide a major innovation, right now, society does a pretty bad job. A large part of that is simply time. If you create something whose value becomes apparent after 20 years or 30 years, we just don't have the mechanisms in place to go back after that period of time and say, "Oh, gee, you did a really good thing 30 years ago. We're now going to reward you in some way." Even if we could reward someone after 30 years, that's a bit late. If I could put in a brief plug for something, I would put in a brief plug for a concept called prediction markets, and you can Google it and find out more.

Plutte: I love the start out, which is, we are not good at rewarding breakthrough, revolutionary. I wonder if you could say something, this is what happened to us. We were too far ahead. People didn't know what was going to be made of this. In some fairly short way so we can use it; it's an important point.

Plutte: Bring it back to your personal and your group's personal experience.

Merkle: Let's see, how do we say this? I think one of the things that we learned from all of this was that society is not really very good at rewarding really visionary advances. I think the primary reason is that really visionary advances are those advances where it's not recognized that it's a big thing until decades later, and society has a hard time dealing with that kind of timeframe. In our situation, we made an advance and it took a long time for this advance to work its way through the system and become actually, directly useful and valuable to a large number of people. There are also a large number of detailed activities that had to take place between then and now, and somehow in all of that process, the connection between the original activity and the contribution that we made got lost in the process. So I don't know exactly how to address this, but it's clear that if you do want to make great contributions to society, then whether or not you get a reward is a bit of a random event.

Plutte: That's good. I like that. Can you paint a picture of how the world would be different today without public key cryptography?

Merkle: I think the major difference in the world today if public key cryptography did not exist primarily would be in the ease of communications and in the ease of authentication of information. It would be more difficult and more expensive to provide secure communications and more difficult to provide authenticated information in this global network that we have. It would still be possible, but it would be more difficult and we'd have to work harder to get it.

Plutte: I have one more question and then I'd like to ask two questions for our exit theater downstairs, which is part of the exhibit at the end. We'll get to that in a moment. About 15 years ago, Sun co-founder, Scott McNealy, claimed "privacy is dead." Is privacy dead?

Merkle: Everyone wants to know whether or not privacy is dead, and that's a very hard question to answer, as someone who has focused primarily on the technical aspects of it. I don't know if I can properly address such a broad question as privacy, which encompasses a huge range of very complex social and other issues. It's something which is very difficult and has a lot to do about what we want to have happen. If we as a society place a high value on this concept, then we can preserve it. If we don't place as high a value on it, then it becomes more difficult to preserve. What will happen, I do not know, and whether or not we can preserve it, I do not know. I know that in a digital age, it is likely more difficult to preserve, but whether or not we do preserve this concept and exactly how we define this concept is largely up to us.

Plutte: That's great. We have an exit theater downstairs, so people look through the entire exhibit, see the history of computing and at the very end, we have a lot of people from the industry, who've been in shorter and longer periods of time, answering a few questions and giving little philosophical pep talk to people in the future. My first question is, what advice would you give to a young person just starting out in a career today?

Merkle: For those who are starting in a career today, I would say that we are seeing major technological shifts and major technological opportunities. Learn a lot about those technologies that are changing most rapidly and where the opportunities lie and be prepared to adapt rapidly. The opportunities are so huge that you will be staggered by the magnitude. You must, you absolutely must, be prepared to focus on those opportunities and pursue them with all of your heart, because opportunities like this only come along, not just once in a lifetime, not just once in a century, not just once in a millennium, but once every tens of thousands of years. We are seeing opportunities in our lifetimes that are going to shape the history of this species on this planet, and beyond this planet. I suggest that you pay attention and take advantage of the opportunities that have been handed to you on a silver platter.

Plutte: That was great.

Merkle: It's true, too.

Plutte: Why do you think understanding computing history is important?

Merkle: Computing history provides us with an easily understood example of exponential progress. Computer hardware provides us with the simplest and the clearest example of what exponential advance means in technology, and that example is going to be applied throughout a range of technologies in the coming decades. And we will see the lessons that we learned from computer hardware applied over and over and over again across a whole range of other technologies.

Plutte: What do you see as the next big challenge for technology?

Merkle: Technology is now advancing along two primary fronts. One is the material front, atoms and molecules, and the other is the front of intelligence, of software, of programming, the front of machine intelligence, if you will. These two fronts are going to be the two major fronts of the 21st century. They're going to be on the one hand, the front that gives us computers that are smarter than humans, which is going to produce a whole range of implications, and on the other front, the ability to control and master the arrangement of atoms and the ability to arrange and re-arrange the structure of matter, so that we will be able to build essentially any structure consistent with the laws of physics and chemistry. Together, these two revolutions are going to rewrite our concepts, both of what it is to deal with the physical world,

and what it is both to deal with our mental world and even what it is to be human. So I would suggest paying attention to both of these revolutions and participating in and understanding both of them, because negotiating and navigating the world in which these two revolutions are going to change everything, is going to be very important, and is going to be the next challenge for humanity.

Plutte: Thank you. I don't have anything else. Do you? We're done. Thank you very much.

Merkle: Cool.

<crew talk>

END OF INTERVIEW

