Silver Bullet Talks with Whitfield Diffie

Gary McGraw | Cigital

Hear the full podcast at www.computer.org/silverbullet. Show links, notes, and an online discussion can be found at www.cigital.com/silverbullet.

Whitfield Diffie is a cryptographer and consulting professor at Stanford’s Center for International Security and Cooperation. He’s worked at MITRE, the Stanford Artificial Intelligence (AI) Laboratory, and Northern Telecom and was chief security officer of Sun Microsystems. He’s best known for discovering the concept of public-key cryptography in 1975, an idea he jointly developed and expanded with Martin Hellman. Public-key cryptography not only revolutionized the crypto field but also changed the crypto community forever.

Long ago, you left your post at the Stanford AI lab to work on cryptography. Can you explain what happened and how you got the idea for public-key cryptography?
In the summer of 1972, Larry Roberts, who was funding ARPANET, went to see Howard Rosenblum of the NSA [National Security Agency] with a very reasonable proposition: “We have a US$100-million-a-year military research project, and we ought to think about security.” I wasn’t in that conversation, but I infer that they agreed but couldn’t settle on the next steps because Roberts didn’t want to fund any secret research and Rosenblum didn’t want to do anything else. Roberts had a job in which his principal investigators had to listen to whatever he wanted to talk about, so that week he talked about network security. My boss, John McCarthy, got excited about the subject. He came to the lab and chatted us up about network security. Several people were interested, but I was the only one who stayed interested.

At the time, cryptography dominated network security in our minds, so I began studying it. Six months later, McCarthy was fed up because the NSA was supporting me with under-the-table money to work on a different problem: proof of correctness of programs. I took an indefinite leave of absence and was terminated after a year. I began traveling around the country. I had originally intended to travel the world but was interrupted by my first discovery—meeting my wife in New Jersey. Without that discovery, I probably wouldn’t have made any of the others.

We began traveling together, and in the summer of 1974, I visited the cryptographic laboratory at IBM in Yorktown Heights. I went to see Alan Titter, who called himself the biggest man in computer science—he weighed 500 pounds. Titter is one of the famous first-generation phone hackers. He introduced me to his boss, Alan Konheim, who was in the mathematics department [at the Thomas J. Watson Research Center]. They made a major input to the development of what appeared two years later as the US Data Encryption Standard [DES]. Konheim was very secretive, and he told me only one thing, and since then, he wished he hadn’t.

He said, “Two people can work on a problem better than one, so you should look up my old friend Marty Hellman when you get back to Stanford. He’s interested in this stuff too.” I got back to Stanford and met up with Hellman. Each of us found the other to be the best-informed person willing to talk
About Whitfield Diffie

Whitfield Diffie is a consulting professor at the Center for International Security and Cooperation at Stanford University. He is best known for discovering public-key cryptography, which he developed along with Martin Hellman in 1975. Diffie was the manager of secure systems research at Northern Telecom in the 1980s and joined Sun Microsystems in 1991, where he became a Sun fellow and acted as chief security officer until 2009. Diffie is a Marconi fellow and the recipient of a number of awards including the National Computer Systems Security Award (given jointly by NIST and the NSA) and the Franklin Institute’s Levy Prize. He is the coauthor of Privacy on the Line: The Politics of Wiretapping and Encryption.

Talking to each other a little better than east and west because north and south can each see one of the hands they’re discussing, whereas east and west can’t see either. Imagine a public negotiation between two people. Observers listen to every bid and every response, but at the end of the discussion, the negotiators share a secret that none of the observers know. That’s the approach that became the Diffie-Hellman system.

Another way of envisioning it is to split the cryptographic key in such a way that there’s an encrypting capability and a decrypting capability, and you can’t decipher one from the other. If I want to send you a message, I go to the phone book, look up what’s now your public key, encrypt the message with your public key, and send it to you. Even though everyone can know your public key and everyone sees the message I sent, only you—the one person who has the private key—can decrypt it.

I was intrigued to learn that you worked with John McCarthy at the AI lab. What were you working on back then?

My fantasy was an automated space station—something you might see in Battlestar Galactica or Deep Space Nine. Objects are constantly coming and going very fast, and if one hits you there will be the devil to pay, so the programs that run the space station really have to be correct. But proof-carrying code has a different view, which is that you don’t try to prove everything, you merely try to prove that the code has certain properties. An obvious one is proper stack management.

My viewpoint would now be called programming methodology rather than proof of correctness, because my view was—and probably
still is—that we can’t write correct programs and prove programs correct because we don’t know how to write programs.

One of things I worked on at the AI Lab that I was pleased with that also interested McCarthy was organizing. I was working on organizing the LISP compiler in such a way that if you didn’t tamper with certain pieces of it, you wouldn’t get stack errors. If you didn’t tamper with a layer below that, you wouldn’t get syntactic errors in the assembly code.

I think that, as a child of historians, you were destined to be a careful thinker. Do you regret not going into academia further, or do you feel like you’re in academia? I regret not having been the greatest thing since sliced bread, but I did what was in my capabilities and limitations. Looking back, I wanted to be [Pierre] Deligne, a Belgian student of [Alexander] Grothendieck and one of the most celebrated names in late 20th century mathematics. I imagined myself solving great classic problems in mathematics. The big thing in [Andrew M.] Gleason’s career was solving Hilbert’s fifth problem; he did problem sets for 20 years or so, and then he had the answer. I felt ill-advised as a youth. Historians talk about historiography, teaching people how history is done, where the sources of history are, what the methods are, et cetera. Nobody ever taught me much about the research world.

I had read Eric Temple Bell’s Men of Mathematics, so in essence I was trying to model my career on 19th century mathematicians. I was looking at a classic vision of mathematics. I learned more and saw a wider world in that direction when I was at MIT [the Massachusetts Institute of Technology], but I really wanted to see things like the Riemann hypothesis solved. Without question, that kind of thing is important, but it’s more useful for a young researcher to see the things that are easily defined in concept.

In my view, a special relativity is a worship-worthy discovery. Who would’ve thought that the problem of resolving Galilean relativity against the constancy of the speed of light was going to be to make time change? That man deserves the respect he gets.

A few years ago, I read Rebecca Goldstein’s biography of [Kurt] Gödel, which contained a statement that every young aspiring intellect should hear: Gödel was determined not to waste his time on any problem that could be solved by lesser minds. Now, that’s really good career guidance. He looked to things and asked, “What are the most important problems?,” and then set out to solve them.

I want to ask you a quasipolitical cryptography-related question. The FBI director, James Comey, seems to imply that he’d like to put some back doors into modern systems for law enforcement reasons, which many of us think is a terrible idea. Why is this a terrible idea?

The bottom line of society is that you bear the consequences of your actions. So, if I know something that the court can legitimately order me to tell them, I can either tell them or go to jail. [American journalist] James Risen is willing to go to jail rather than to reveal his source because he thinks the right and the power of reporters to talk to sources and protect them is indispensable to the news business and to democracy.

Comey wants to take away that choice. The state can always take any information you have without your permission, so that you have no freedom to refuse the state anything. That’s a relatively new notion.

So, privacy of communication had certain limits, but there was a solid privacy of face-to-face communication, which was the most important mode of communication at that time.

Since the 20th century or so, remote real-time communication has become feasible and has risen to challenge face-to-face communication as a component of culture. You and I might never meet, but we can talk very satisfactorily on the telephone. Some people in society never meet the people they work or otherwise communicate with. We can expect that, as communications improve and we go from kilobaud to terabaud, the occurrence of these remote encounters will be greater and greater.

If remote communication must be accessible to the state, society will have an awful bug—it can move away from freedom in a way that can’t be corrected.

I was at MIT [the Massachusetts Institute of Technology], but I really wanted to see things like the Riemann hypothesis solved. Without question, that kind of thing is important, but it’s more useful for a young researcher to see the things that are easily defined in concept.

In my view, a special relativity is a worship-worthy discovery. Who would’ve thought that the problem of resolving Galilean relativity against the constancy of the speed of light was going to be to make time change? That man deserves the respect he gets.

A few years ago, I read Rebecca Goldstein’s biography of [Kurt] Gödel, which contained a statement that every young aspiring intellect should hear: Gödel was determined not to waste his time on any problem that could be solved by lesser minds. Now, that’s really good career guidance. He looked to things and asked, “What are the most important problems?,” and then set out to solve them.

I want to ask you a quasipolitical cryptography-related question. The FBI director, James Comey, seems to imply that he’d like to put some back doors into modern systems for law enforcement reasons, which many of us think is a terrible idea. Why is this a terrible idea?

The bottom line of society is that you bear the consequences of your actions. So, if I know something that the court can legitimately order me to tell them, I can either tell them or go to jail. [American journalist] James Risen is willing to go to jail rather than to reveal his source because he thinks the right and the power of reporters to talk to sources and protect them is indispensable to the news business and to democracy.

Comey wants to take away that choice. The state can always take any information you have without your permission, so that you have no freedom to refuse the state anything. That’s a relatively new notion.

So, privacy of communication had certain limits, but there was a solid privacy of face-to-face communication, which was the most important mode of communication at that time.

Since the 20th century or so, remote real-time communication has become feasible and has risen to challenge face-to-face communication as a component of culture. You and I might never meet, but we can talk very satisfactorily on the telephone. Some people in society never meet the people they work or otherwise communicate with. We can expect that, as communications improve and we go from kilobaud to terabaud, the occurrence of these remote encounters will be greater and greater.

If remote communication must be accessible to the state, society will have an awful bug in the sense that it can move away from freedom in a way that can’t be corrected. To paraphrase [lawyer and politician] Frank Church, if the intelligence community can turn its power on the American people, there will be no freedom and no way to restore democracy. I think that looks very prophetic at the moment.

Me, too. You were working at Sun when Scott McNealy said privacy was dead, were you not? There certainly was a lot of truth
to that. It’s a very difficult problem to solve because, in one sense, it’s clearly gotten worse since then. Imagine you have a spaceship that’s 1,000 kilometers across, but if you speak a person’s name, they can hear you from wherever they are. So, there’s no privacy: the spaceship tracks where everybody is, and knows who knows whom.

If you have trust, or if you put aside the issue of trust, this situation offers all sorts of wonderful things. It’s great to have systems tracking you so they know where to find you when you want to be found. For instance, they can tell you which restaurants are local. All these things that Google and others are either doing or developing are immensely useful.

The problem is that the word privacy doesn’t express the difference between the things you want and the things you don’t want. People say things like “there’s no privacy in small towns,” and in a large sense that’s true. Small towns have a lot of accountability because the people who know about you are people you know about. They’re not capriciously going to offend you because they’re just as vulnerable to you as you are to them.

On the other hand, ChoicePoint and Equifax and such couldn’t care less about us. We have no visibility into their operations, and they have a lot of visibility into ours, so there’s that asymmetry of transparency in which the individual is transparent to the large organizations, but the large organizations aren’t accountable to the individuals.

Yeah, it’s a thorny thing. Thanks for your time today. It’s been incredibly interesting.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital and this magazine and is syndicated by SearchSecurity.

Gary McGraw is Cigital’s chief technology officer. He’s the author of Software Security: Building Security In (Addison-Wesley 2006) and eight other books. McGraw received a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him via Twitter @cigitalgem.