**Mapping the Journey, Episode One.**

**Interviewer: Pramod HS**
**Interviewee: Rich Salz**

**Pramod:** Hello listeners, Pramod here, welcome to the first ever episode of the Podcast "Mapping The Journey." Here we unmask the people who are making tremendous strides in tech and yet whose names and stories are seldom heard. This week we will be following the journey of Rich Salz. He is currently working at Akamai Technologies, OpenSSL core team member. He's a pioneer in the field of distributed systems and security. He has been involved in definition and implementation of standards for more than 20 years. Let's hear from him. Rich, welcome to the show.

**Rich:** Hi there, nice to meet you and talk with you.

**Pramod:** Yeah, so you studied at MIT, computer science what were you focused on?

**Rich:** Okay it was it was a very long time ago.

**Pramod:** Just curious to know, like how was it to study back in the 1970s and 80s?

**Rich:** Yeah! So some of the freshmen programming classes for like mechanical engineering they had to write their programs in Fortran on Punch Cards. This was even before Kerberos and X at MIT Athena, so it was minicomputer programming in ALGOL and so on. Towards the end of my studies, I started to do some more lisp and scheme work, and of course, it's all very different Java, Python and so on.

**Pramod:** Okay, so another interesting thing, you were also an editor-in-chief for the tech MIT'S oldest newspaper, I saw your name.

**Rich:** Erm yes, good research. Yeah, I was in the newspaper high school, I think information flow and putting things out there was important, so I like newspapers. I worked at the newspaper for all my time at MIT, probably spent more time and was more successful at the newspaper than I was in my classes.

**Pramod:** That's nice, okay. So then you worked with USENET, distributed discussion systems for a long time, can share your experience there?

**Rich:** Sure! So one of the things I like, so this was even before open source was really a term, we had certain newsgroups that were moderated and then I became as a way of volunteering on to give back. I became the moderator of the source newsgroup 'mod.sources' that distributed source code, and it was, for example, the first four-five versions of Perl were distributed that way, and a whole bunch of early games and things like that were was just UNIX systems connected via dial-up lines. It would pass things around from doing the moderating, and then I got involved with an Internet version that I wrote, it's called INN because our

systems were getting hammered by how inefficient it was. It was also part of the same sharing source code sharing ideas and so on that drove me.

**Pramod:** Okay, so people were really starting to realize the benefits of sharing information digitally and also they wanted to discuss globally?

**Rich:** Yes, there was after a couple of years, there was this effort called the great renaming, which was an attempt to group the newsgroups from flattening space into top-level categories. Like science, maths, moderated newsgroups, source control stuff like that UNIX oriented and so there was a lot of discussion groups, and then there were the technical groups because at this point you know, people were paying to deliver all the stuff with modems 1200, 9600 baud, sometimes 19.2 KB. So they want to be able to prioritize traffic especially dialing long distance phone calls, transfer things over to Europe and so on. There were these long discussions, sometimes heated but USENET was also where the first the term frequently asked questions (FAQ) came out and were also the very first spam was issued. On were some lawyers were posting about green cards and their services. So it was very much like community discussions we have today on social media, but it was a much smaller select group because it was pretty much restricted to technical people who ran UNIX systems.

**Pramod:** Okay that's interesting FAQ's and spam, never knew about that. Then you joined OSF, what was your motivation? Just for the listeners, it's an organization founded to set up standards for implementation of UNIX.

**Rich:** Sure, so I was working at the time at BBN, which was an early networking company and then wanted to move out into some other less government-sponsored research and more commercial things. OSF was created by a bunch of companies who wanted to come up with a common UNIX platform and then a common user interface that was called motif. There was also a version called CDE the Common Desktop Environment. I worked on something called DCE the same three letters shifted which is distributed computing. It was sort of a response to Sun RPC or a predecessor, for what we might think of as the WS web services stuff, that got overtaken by REST, but you know WS security. So DCE used Kerberos to make remote procedure calls and to build. The intent was enterprises could build applications in a secure distributed manner, and that got completely overtaken by the web that became the predominant factor there.

**Pramod:** Okay, so it was more like a setting up standards right for the distributed computing in those days?

**Rich:** It was a setting of standard plus there was also a reference implementation so that somebody could implement the standard purely from the specification or they could license the code from OSF. So for example in the DCE case, Microsoft's DCOM was a complete implementation of DCE purely based on the standard or as everybody else's DCE offerings was using our reference code. I worked on the source code and was a technical lead on helping get other contributors in the other companies to set the technical direction.

**Pramod:** Okay, so you have contributed to HTTP. So today internet is built on top of it, RFC 1945, published in may 1996. So what's your contribution that's very interesting to know there?

**Rich:** So BBN was an internet company, distributed company that one of my close friends set up. The first Web server at BBN and I were just interested in it as a distributed application, you know client server thing over the Internet, and so I did a lot of technical review of the specification. I don't remember things I found, yeah it's been too long but a lot of low-level technical fluff in knits kind of things. I also did some work on the HTTP 1.1 and had been involved with the IETF for a very long time.

Pramod: Okay, So you did a lot of work on distributed systems. When did your focus shift to security?

Rich: From the beginning, I was always interested in the security issues that come up. We have two programs talking, on the one machine that's pretty easy to make easier, to make secure. But when I'm talking to a machine that's over the network be it on a local net or over the Internet it's a lot harder, and they bring a whole other set of problems with it like how I can identify you? How can I authenticate you? I was an early adopter of Kerberos within some applications at BBN which solved a lot of those issues having gone to MIT and working at Cambridge and maintain close contact. Dan Geer is a friend who is the technical lead for Athena. So it's an evolution it's expanding the set of problems right, and we still have those problems on the net it's a natural way for me to move from distributed security to TLS and web security or what we call the web PKI, the web public-key systems certificates in CA's and so on. So it's always from the beginning I've had it, and it's a sort of following the industry to stay relevant and help make useful contributions I hope.

**Pramod:** Okay so today you are OpenSSL core team member, it's the most widely deployed TLS library. When and how did you get involved with this OpenSSL?

**Rich:** Sure at the time I had been working at Akamai for about a year, we got an early notification about this thing that looks like it was a bad security vulnerability. It became known as the heart bleed. One of the talks I said, it was more popular than the Kardashians at one point. After heart bleed, we at Akamai have a whole bunch of patches we've done for the 14 years before I joined including some secure memory allocation stuff that would have helped prevent it. Shortly after heart bleed came out and it was all fixed, the team reached out to me personally and said we would like you to join. So at that point, before heart bleed, they were like two people working on it, after heart bleed we now have about a dozen, and we are hoping to get more committers. So that was the genesis, they asked me Akamai approved, Akamai told me to spend a portion of my time working on OpenSSL for the benefit of the Internet and also for you know the benefit of Akamai.

**Pramod:** Okay so how does the development takes place so who raises the issues and what are some of the challenges?

**Rich:** Sure, OpenSSL for a long time the challenges were that the project was sort of walking

dead. There were two people working on it nobody was funding it; they had to take other consulting contracts to like Phipps work, federal standard Phipps version of OpenSSL to pay for the stuff. So there was a problem that there were a whole bunch of open bugs. Nobody ever looked at, or book reports. There was no way to get code and enhancements into the system. Because the people were just too burnt out and too overloaded so and that people were just starting to fold up their hands. One of the things that we did is we helped to re-energize the community, people then started to do more things on Github. It took a while, but at this point, except for security fixes, everything is done on Github now. And frankly some of the people who were involved in the heart bleed, it took them a while to feel comfortable doing that. This is because there's a lot of jerks on the Internet, and they don't want to put code out there with their name on it closely attached, and the people say "oh you the stupid idiot, how could you do that blah blah blah." So it's as I said there's a lot of jerks on the internet, there's also a lot of good people. So we have more what we call transparency, developed by-laws, we have posted them we everything except everything like I said security is done on Github. We have made a really strong effort to get people to report bugs. I had done a lot of work going through and closing old invalid bugs we finally closed the bug database and moved it to get converted it to Github issues and so on so. I think when people see you are interested in their input when people see that they can make contributions, we have hundreds of Pull requests, we've merged. Many of them I don't know what the percent would be but a maybe a third come from people outside the team, where people can report issues and bugs and the team will respond. It builds up this virtuous circle where you get more contributors and more involved and so on. We still do maintain believe that we are the most useful and most widely used package out there and we are trying to keep up that leverage that effort. We have made partnerships with a couple of computer companies. Intel has been a sponsor, and Oracle's been our sponsor. Akamai pays for me, and various other people employed the core infrastructure initiative gave a lot of money because they came out after heart bleed gave a lot of money to help fund OpenSSL and show the importance of open source security software packages.

**Pramod:** It's really nice to know that because I think more than 35% of the traffic goes through OpenSSL.

**Rich:** Oh yeah!

**Pramod:** Nice that people are thinking.

**Pramod:** Yeah

**Rich:** Yeah

**Pramod:** Another thing I wanted to know is, you're part of many security reviews, I wanted to know what's the process is like. Could you shed some light on who proposes and how are they reviewed?

**Rich:** For OpenSSL stuff or in general?

**Pramod:** No, in general, Iike RFC's when studying computer science.

**Rich:** Right okay, so the IETF it's a website with a bunch of mailing lists right, and they write documents and eventually become standards are proposed its code RFC's. The IETF is divided into a number of areas. I work as you might guess in the security area and one of the things each area tries to do is at least have somebody review every document that comes out, so it covers a wide range of industry expertise that gets looking at it. So when the security group does its review and yes I've done a lot of it's called sector of the security directorate. We look for things like the protocol looking at the is the protocol itself secure or does it say for example well to set up a session send your name and password over to the other side, less clearly not secure. You send an encrypted password you have to have some understanding of cryptography and the techniques and that you just get being in the history for a while. Then think about what can happen if one site is down or what can happen if somebody steals all of the traffic right. Can they, later on, decrypt it?or can they, later on, impersonate on one side of the other? So then you start to think of things like well maybe the protocol should have a validity period. And that's like a certificate has it not before not after, time to live just the way like also the way DNS cache work. So just have to bring your experience, and your background while you read it and you sit there and make some notes on the side. And then write it up and send to the authors who would almost always in my experience always very receptive to the feedback you give because everybody wants to get you know the best possible documents out there.

**Pramod:** Yeah! You generally give feedback they fix it and then send it back to you again for the review. That's like a process.

**Rich:** Yes, the reviews I've given have been very well received, and I think I have helped to improve the documents and the authors understand that too, especially cause most of the people working on these things are not security people.

**Pramod:** So one last question you have been involved in the definition and implementation of internet security standards for more than twenty years now. What is your contribution that you are really proud of or want to share with us?

**Rich:** Oh that's an interesting question, so I guess the thing I'm most proud of is helping to revitalize OpenSSL. I was on the outside during the early days of OpenSSL where we'd submit, and people I worked on did some pretty fundamental core patches that got accepted. I was there watching while it went downhill and almost died and then I was part of the team that brought it back to life. So I'm most proud of that contribution that the that USENET stuff, it's time was really cool and fun. The world and the web swamped everything else and so the fact that OpenSSL is still or is once again a very important and vital security technology and that it's freely available and relatively easy to use. That's great, and that's the most important thing. The second most important thing is my company's a sponsor of let's encrypt which gives free certificates and so that's also really important. Security on the web and privacy on the web and knowing that you are talking to the Web server you intend to be talking to are all very important.

**Pramod:** Okay. Thanks for all your contribution to the field and thanks for being part of the podcast it was an absolute pleasure talking to you.

**Rich:** It was my pleasure and my privilege, and I look forward to seeing the final link so I can tweet it around on social media.

**Pramod:** Yeah definitely.

**Rich:** Thank you, bye.