The Cybersecurity of Quantum Computing: 6 Key Areas of Research

Featuring Thomas Scanlon as Interviewed by Suzanne Miller

Welcome to the SEI Podcast Series, a production of the Carnegie Mellon University Software Engineering Institute. The SEI is a federally funded research and development center sponsored by the U.S. Department of Defense. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

Suzanne Miller: Welcome to the SEI Podcast Series. My name is Suzanne Miller. I am a principal investigator in the SEI Software Solutions Division. Today I am joined by Dr. Thomas Scanlon who leads the data science program in the SEI CERT Division. Dr. Scanlon recently participated in the Workshop on Cybersecurity of Quantum Computing co-sponsored by the National Science Foundation (NSF) and the White House Office of Science and Technology Policy. Participants in the workshop examined the emerging field of cybersecurity for quantum computing, which is the topic of today's podcast. Welcome, Tom.

Thomas Scanlon: Thanks. Great to be here.

Suzanne: You have done podcasts with us before, and we will include links to those for our audience. But for those members of our audience who haven't listened to your previous podcast, could you start by just giving us a little bit of what you do here at the SEI and what's the best part about your job?

Thomas: Sure. I am currently the technical manager for the CERT Data Science team. We are looking at areas where cybersecurity and data science intersect. So it is about protecting AI [artificial intelligence] and ML [machine learning] systems and using AI and ML systems to solve cybersecurity problems. As part of my team, we also have quantum computing in our area, which is what we're going to talk about today. So we are looking at a few different aspects of quantum computing which we'll talk about today.

Suzanne: Yes, and especially the cybersecurity aspects of it today. We have done previous podcasts on quantum computing with various members of your team. For those in our audience who haven't heard those podcasts or haven't heard of quantum computing, we will include links in our transcript. But can you give us just a brief overview on quantum computing and how does it differ from what we might call traditional binary computing?

Thomas: Sure. Typically, in relation to quantum computing, we say classical computing to talk about the traditional computing you mentioned. But in a classical computer, information is stored as a one or a zero as bits, and those bits are reflective of a physical property that a transistor has current to it or not. With each bit, we can represent one piece of information. The bit is either on or off. In the quantum world, we use something that is called a qubit, and that can store more information. I have a little bit simplistic example but it really resonates with people. I think of flipping a coin in the air. And so, if you flip a coin in the air and it lands heads up or tails up, you can then measure it heads or tails and that's similar to measuring a one or a zero in a classical computer. However, if you can measure that coin while it is flipping through the air, it can be in the state of one and zero at the same time. That is sort of what is going on in the quantum computer. We have something called superposition, and in superposition it allows the qubit, which is the term we use, allows the qubit to represent one and zero at the same time. Then another property of quantum computing that allows us to store more information is this concept of entanglement. But in this example, imagine you could flip two coins at the same time and measure both their states at the same time in relation to each other. So now, you can store more information. As you add qubits, the ability to store information grows exponentially. On a traditional computer, it grows linearly. So, as you add bits, it grows linearly. But in a quantum computer, it grows exponentially as you add qubits.

Suzanne: That is really the attraction of quantum computing is this ability to store more data related to attributes that we care about that we are using in our software. That is one of the things that really comes through to a lot of

people is that we actually get some advantage from quantum. It is not just a toy, *Ooh, isn't that cool that we can have superpositions and entanglement?* But it actually has meaning in terms of our ability to include more information. As we get into the AI and the ML and the big data, that becomes relevant, right?

Thomas: Yes, so it allows us to represent more data and allows us to do calculations on it. What we talk about is that in classical computers there are untractable problems. Sometimes you may hear the term NP-hard problems. The problem is not that they can't be solved, it is that they can't be solved within human reasonable time scales with the computers we have available to us today. Due to the potential of quantum computers to process information much faster and much more information, that will allow us to solve problems that would be untractable today.

Suzanne: Talking about sort of the bigness…big data, data science, is your specialty area. Where did quantum computing and data science explicitly converge?

Thomas: There is a field of research on quantum AI and quantum machine learning. Really, anytime you are doing data science, most of the time anyway, you have a lot of data that you need to work on. That is why you are using AI or ML in the first place is to process a lot of data and make a prediction about something. With the power of quantum computers, there are machine learning algorithms, different approaches that you might not try today because you couldn't get your results in a reasonable time. If you have that power of a quantum computer, that can really accelerate the types of problems you can also solve in the AI and ML world. So there is a relation. One of the areas, that that research is looking at is…quantum computers are used now and probably will be in the near future is as what we call classical-quantum hybrid. You are still going to use a classical computer to do a lot of tasks, and then the quantum computer will be more of like a coprocessor where you will form out the calculations. Given that, when you are talking AI and ML and lots of data, there is a bandwidth problem to be solved on how do I get all this data from the classical world to the quantum world. That is one of the many challenges in the quantum computing space that folks are working on.

Suzanne: OK. With more data come more threat surfaces, attack surfaces, and threat vectors. You talked about this in a recent blog post and the aspects of quantum computing that make it a potential target for malicious actors. How did the attack vectors in quantum computers differ from attacks that are leveraged against classical computers?

Thomas: Yes. This is an area that, as you mentioned, I have been working with some other researchers around the country on. The idea is the most press that quantum computing is getting is threats it may represent to cybersecurity, its ability to break encryptions and do things like that, but there hasn't been as much discussion on how to protect quantum computers. Anyone who works in security, we always want to be in sooner, right?

Suzanne: Sure.

Thomas: There are network protocols in use today that weren't designed with security in mind. They were designed with functionality in mind. Since we are still at the advent of quantum computing, now is the time to start thinking about security and really get security concerns addressed up front. Some of the differences are... a lot of the threats that are in classical computers will also be in quantum computers, first off.

Some of the things that are different is given the amount of resources it takes to perform a quantum calculation and get a result, the protection of that result is going to be even more heightened than normal. So, in a classical world, if I could get access to your data, I could probably recompute results on my own and draw conclusions. But because of all the horsepower and resources that go into creating a quantum result, I am going to have to take your result.

Suzanne: I don't want to have to recreate the data. Yes. OK.

Thomas: Another difference is the sensitivity to the physical environment in current quantum implementations. And so, it is more sensitive to heat and noise and environment. I can perform essentially a DDoS attack or some type of attack on your quantum calculations by attacking your heating and cooling systems. I can attack the integrity of your quantum calculation by introducing noise. So there are some different attack vectors for quantum computers that need to be researched and solved.

Suzanne: Given that, how do people using quantum computers protect themselves from these types of attacks? Do we have strategies in play already, or is that sort of something that was really part of what you were exploring in the workshops?

Thomas: That is part of what we are exploring in the workshops. We looked

at things that have been done for inspiration. There are parallels to high-performance computing and the protections for those that would apply to quantum, but there are also some things that need to be uniquely developed for quantum. This gets into the six areas that we outlined in the blog. But for instance, there isn't, for existing quantum implementations, the ability to monitor processes and progress the way there is for a classical computer. I can pull up and look at CPU utilization and figure out which jobs are using which horsepower, and even sort of infer what types of activities they are doing. In the quantum world, we don't have that tooling and instrumentation right now. That is one of those six areas of research.

Suzanne: That applies not just to security but just to understanding whether what you have asked the computer to do is taking up too much bandwidth and too much resource. You need a task manager in the Windows equivalent world so that you can understand multiple aspects of your quantum computing, but security certainly would be one of them.

Thomas: Absolutely. And also, another attack that someone might want to perform a quantum computer is just hijack your quantum computing power. I don't have quantum computing power of my own so you think of an analogy to like how botnets work in the current world. I want to hijack your computing power and perform my calculation. Currently there are no reliable methods to say what algorithms the quantum computer is working on. You wouldn't necessarily know that some unauthorized algorithm is being executed in your quantum. These are all the areas of instrumentation and control systems that we definitely need research in.

Suzanne: What are a couple of other areas? You mentioned six areas. We have got the sort of botnet, *I'm going to hijack your computing power*. I have got the, *I am going to mess with your HVAC*. [Another area is] *I am actually going to try and hijack your result*. What are some of the other areas that you are working on?

Thomas: Two related areas that we called out in the workshop that are described in the blog is creating formal methods for safe and secure quantum computing systems and developing the tools needed to verify quantum algorithms. There is a relation there but, as you know, there is a lot of work in formal verification software and applying formal methods. Just like I talked about earlier, we have parallels between high performance computing and quantum. We have a lot of rich history to draw on informal methods of verification of software systems, but we need to grow and adapt those for the quantum space, so that we can provably prove things about

quantum computers.

Suzanne: One of the challenges of that has got to be that at least most of the formal methods that I am aware of have really been focused on deterministic kinds of proofs. In the quantum world, you are dealing with probabilities. Many of your sort of outcomes are probabilistic. Is that one of the challenges in adapting formal methods?

Thomas: That is a challenge. Quantum computers can solve deterministic problems.

Suzanne: Of course, yes. But they can also solve the probabilistic ones that the other classical computers can't.

Thomas: Right, and so, that is part of the discussion is, what formal methods will apply more directly? Where are areas for future research. Maybe if there are areas where we can't develop formal methods, what is the best we can do to try to maybe probabilistically prove a property. That is an area of research too.

Suzanne: OK. If I am trying to work in quantum right now, probably security is not at the top of my list of things I'm worried about even though I should be. What are the first couple of things I should be doing to protect my system from what we have available to us now?

Thomas: Yes. I do look at the quantum cybersecurity that we are talking about today as a little bit of a future task for users of quantum computers. It is something that needs to be addressed now by developers and researchers and implementers. If I am an organization that wants to leverage quantum computing, or be positioned to leverage it in the future, one of the first things that I tell folks to do is develop quantum use cases. In your organization, talk about problems you have that a quantum computer might be able to address, talk about where you would get data to address those problems, talk about what success would look like in those use cases, a lot of typical use case development things. As you work those quantum use cases and you think about how you would use quantum in your domain, then you can start to ask, *OK, if I do use quantum in my domain, what do I need to protect? How do I protect it?* Then you want to start having the security discussion now. For the same reason, if you are a pharmaceutical company and you develop…One of the areas for promise for quantum computing is in chemistry. If you use quantum computing to develop some new drug or biology, some new molecular combination or something like that, now, you come back to those

questions I raised earlier: *How do I protect this result? How would I be able to verify my results? How do I protect my calculations?* You also get into some regular software engineering problems like, *How can I recreate my result?* But if you can recreate it, that also helps speak to the security reliability.

For the average organization that is not a firm developing a quantum computer, I think you wanted to start with quantum use cases and say, *What would we do with quantum*? And, *What are our realistic problems for quantum?* That may be somewhere you want to consult with someone that knows more about quantum to say, *Hey, these are good use cases*, or, *This wouldn't make sense.*

Suzanne: Yes. To the security point, as you work through those use cases, you start to get an idea of what are the assets I need to protect as you said before, *Is it the data or really is it the result? Is it the algorithms? And then, how do I go from there?*

Thomas: Yeah. And so, another part of that for like end-user of quantum computers is it is, you know, fairly feasible that when quantum computing becomes available to a typical organization, they're going to use it as some type of cloud service, either a cloud proper or cloud as a concept. But it is going to be like a shared service. Most organizations in the near future or even the sort of mid-future aren't going to be bringing their own quantum computing environments in-house. Some will, but most probably will not. They will just want to use the processing power. Then you have to talk about *How do I get my data in and out of there? What are my multi-tenancy requirements?* So, whom I am willing to share this computing cloud with. Some of these issues, again, that are sort of relevant to cloud computing now, but do it in a quantum context. *Will someone else's use disrupt my calculations?* You know, those are questions you might want to ask.

Suzanne: Right, right. All right. Those are all good questions. I think people will appreciate hearing those. But there is a little bit of, on the end-user side, sort of stay tuned, we are really at the beginning of this. We don't really have the frameworks in place like we have for classical computing for cybersecurity folks that are trying to do the protection at the endpoint.

Thomas: Yes. We are entering an era that in the quantum computing literature we call NISQ (noisy intermediate-scale quantum era, which is noisy intermediate scale quantum computing. The idea is it is intermediate scale. We have some quantum computing power. We have some qubits available. We are nowhere near realizing the full potential of quantum, but we can do

quantum calculations. The noisy piece is that the calculations may still be subject to destabilization and different things. We will have to pay attention to error correction and integrity of the calculations and things like that, so that they won't be provably 100 percent reliable every time. But they are good enough that we can actually compute some things. As that NISQ era comes that is when organizations might want to start to be able to see what kind of problems they can get into solving.

Suzanne: Yes. This is exciting. This is not the only thing you do. You are looking at data science in general. What is next for you? What are you working on now that we will be able to talk to you about in six months or a year?

Thomas: Yes. I neglected to answer one of your opening questions, which is what do I enjoy about working at the SEI. Definitely, what I enjoy is the variety of work and challenges that we get to address here. I have a lot of challenges that are on my plate that we are working on but one— not necessarily related to quantum computing but could be enabled someday by quantum computing—that I have been doing some work in that I am really excited about is measuring trust decay and trustworthiness in a variety of systems.

Suzanne: Oh, interesting.

Thomas: The short of that is there is a lot of tension being paid to zero trust right now for instance. In zero trust, what we really mean is zero implicit trust. We don't trust anything by default. At some point though, we do trust something after we put them through an off-off process, but how does that trust decay over time? I have authorized a device on a network, or you, as a user, sort of naive approaches to trust decay that we use now is basically lapse of time. After so long, I'm going to make you reauthenticate, or maybe…

Suzanne: Yes, you do.

Thomas: Yes. On a VPN, maybe if you drop, I'll make you reauthenticate or something like that. We are looking at this in IoT worlds and 5G communication worlds and say, *OK, someone's coming on and off the 5G network, when is it time to make them reauthenticate?* We are developing probabilistic guesses of somebody is who they say they are or they're not. That can be based on latency, battery power, how often you are on and off the network, physical location, a whole variety of factors and we are applying this in different domains and saying, *Can I make some probabilistic trust*

assertions about whether you belong on this network or in this system or not?

Suzanne: OK. All right. That is interesting. I work in some areas where that would be very relevant. I am sure a lot of our listeners do. That would be something I look forward to talking to you about in the future.

Thomas: Absolutely. That would be great.

Suzanne: I really wanted to thank you for talking with us today in this area of quantum computing. You have talked about us being on the cusp of a new era. It does feel like that. Between the quantum computing, the sort of reduction in the cost of high-performance computing, all the other, AI/ML, large language models, and everything. There are a whole bunch of things coming together. I think quantum computing is going to be one of the enablers for some of these other things that we are starting to get to know what we can do with to actually be able to be used productively. This is really important and keeping that secure is very important to all of us. I think most of us have got the message that any new thing, we have got to get secure.

Thomas: Right.

Suzanne: And quantum fits into that. I am going to be looking forward to what you do in this area in the future. We have the podcast on quantum computing. We have your blog post on cybersecurity. All of that material will be in our transcript today. I want to remind our audience that our podcasts are available in lots of places, [including] Spotify, SoundCloud, Apple, Google, you name it, and the SEI's own YouTube channel. If you like what you see and hear today, give Tom a thumbs up. I know he'll appreciate it. I want to thank you again for joining us and everybody, have a good day.

Thomas: Great. Thank you.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.