The Magic in the Middle: Evolving Scaled Software for National Defense

featuring Tom Longstaff and Matthew Butkovic

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.

Matthew Butkovic: Hello, and welcome to the SEI Podcast Series. I am Matthew Butkovic. I am the technical director for Cyber Risk and Resilience in the CERT division of the Software Engineering Institute. Today, I am joined by Dr. Tom Longstaff.

Tom Longstaff: Hey. Hi, Matt. How are you doing? Call me Tom.

Matthew: Tom is the chief technology officer for the Software Engineering Institute where he oversees our work in cybersecurity, software, and artificial intelligence (AI). Today, Tom will be covering a number of topics. We like the audience to get acquainted with our guests. You are one of the folks that spent some time at the SEI, left the SEI, and then came back and rejoined us. Could you maybe talk about your path to the SEI the first time and then the path that led you back to the SEI?

Tom: Sure. I always like to say, it is better to be in the right place at the right time. I have a career being in the right place at the right time. You might remember back in the late '80s, 1988, we had a couple of really big internet problems, an internet worm that was out there either called the internet worm, or The Morris Worm, or things like that. I was at the Department of Energy's Lawrence Livermore National Laboratory, and at the time getting my PhD, in strangely enough, automatic programming. I also knew a lot about security and a lot about the systems. So when we had this incident, I got onto the team about how to handle this and that rolled into being a technical director in the First Department of Energy Incident Response Team, formed at about the same time the CERT was formed here. I finished my PhD. In 1992 I got called by the SEI to come and basically start a research part of CERT. The idea being, *We got all this data, what are we going to do with it?* That was where I came into CERT for the first time. I spent from '92 to 2007 in startup mode. I kept starting up different kinds of elements all the way through CERT: insider threat, looking at risk analysis, looking at all of the various parts of research that we might do, starting the CERT Analysis Center, getting all of these things cranked up, and then finally ending up as the deputy director at CERT for technology, which was a great gig, an absolutely fantastic gig.

Then in 2007, I got a call from Johns Hopkins Applied Physics Lab saying, *Hey, do you want to come be the cyber advisor here?* I went to Johns Hopkins for 10 years and again, right place at the right time. It was a moment where the intelligence community was really stepping up to a lot of the work that we now look at in the software world and in the cyber world. It allowed me to broaden my horizon into acquisition, broaden my horizon into, *What does it mean to actually do contracting and do the kinds of elements that allowed us to create secure software*? Then, finally, I ended up as an IPA at the National Security Agency in research, looking at this from the government's side. After all of that and it came down to, we were doing searches for the CTO position here at the SEI. I got a call one day from basically the recruiter saying would I mind if they put a package in for me. I literally laughed at them. I said, *Look, I was at the SEI for a long time. They know who I am. There is no way they are going to want me there as the CTO*. And they said, *But we would like to put the package together*. The more we went on to talking about what it would be, the more I got really excited about where the SEI was moving in cyber, software, AI, all of that system moving forward. Finally I said, *Yes, this sounds like a fantastic place*, again, right place at the right time to be. That is how I ended up here as the CTO.

Matthew: Thanks, Tom. I think about the expanse of roles you have had: chief scientist, chief technology officer. One of the things that I think is common is needing to predict or anticipate where technology is headed and then the needs of our stakeholders, in our case, the Department of Defense [DoD]. Tom, in that spirit, I was hoping you could tell us a little more about the status of software and where you think it is headed and the work of the SEI in support of our DoD sponsor.

Tom: First of all let me say we are in a very special time for software, and I don't say that lightly. This is not business as usual with regard to where software is and where it has been going. It is 30 years in the making. It has come to a real head right now where there is no system anywhere in the government, outside of the government, in anything that we touch that isn't software enabled. Software is the key to the entire future of where we are going to go technologically. It has gotten to the point now where not only is that recognized, but now we actually have the challenge of making sure that those software-enabled systems that are out there are trustworthy, are safe, are scalable, and really give us the kinds of capabilities that we need moving into the next dimension. We have always got this thing, right? You have heard this: *You can have it cheap, fast, or good*.

Matthew: Yes.

Tom: Right? Well, and it was cheap, fast, or good, pick two. In the world that we are in right now, we cannot do that. We actually have to have affordable, timely, and capable, and we must have all three. We must have all three going at the SEI. My job is not about predicting the future, strangely enough. It is not. It is really about understanding where the trends are right now and what do we have to invest in to make sure that no matter what happens in the future, we are ready for it, and we are ready to address the issues that are going to happen. Twelve months ago, nobody would have been able to predict some of the areas that we are in in artificial intelligence, some of the areas that we are in in software, some of the areas we are in with DevSecOps. But twelve months ago, we were already preparing ourselves to be ready for this moment. That is my job is to make sure that we, the SEI, and the broader software community, are ready for whatever moment comes.

Matthew: Tom, if I can ask a follow-on question. You describe very succinctly and compellingly the three legs of the stool in software. Is one of those elements more difficult than the other two to achieve? What are your thoughts on the relative difficulty of becoming proficient and trustworthy and robust using those three dimensions?

Tom: The overlap between these means that you cannot actually tease them apart. You can't choose one or two. You must do all three within the processes. A lot of what we have been doing here at the SEI is working to the future of both software acquisition and software development and software deployment through test and evaluation and all the way into continuous ATO, the continuous authority to operate. All of that has been basically using the balance between all three of those items to make sure that we get that capability in the hands of the people who need it quickly, affordably, and capably as it kind of moves forward. That is the goal. Anything short of that is not going to be effective.

Matthew: It is interesting you describe this watershed moment, in essence, which is maybe an overused term, but it really does feel like it is different this time, and that there is a sense that agility and flexibility are the new keys. It feels to me, as someone that is observing this at some distance in some areas, that the idea that things are more temporal than they have ever been is really important. I was wondering if you could speak to that, the nature of software being more quickly iterated and less sort of enduring and monolithic than maybe 25 years ago.

Tom: This is the Ultra-Large-Scale Systems report. In 2006, one of the things that we looked at was the development of really large-scale software systems and what would it take to be agile in a world where the systems are too large to replace. These systems are so large, as we described in this report, that you could only incrementally improve pieces of them at any given time, that you could never take the system down, and you could never actually evolve the entire system at one time. This is the world in which we live, so when you talk about sort of the agile system, let me draw a thread from here to our more recent study in *What is the future of software engineering?* This future, which talks about artificial intelligence and talks about agile and talks about flexibility, talks about how do we create the research to allow us to achieve everything we talked about from 2006 in ultra-large-scale systems? How do we get there? How do we actually say, *Pick a piece of the system, evolve that piece of the system, integrate that piece of the system, while maintaining the capability, affordability, and timeliness that we need moving out there*? Now, if that sounds kind of familiar, it is, because what is now happening in all of these systems is, as we are looking out to replace these, unanticipated by a lot of people were the ideas that every time you get into data-heavy systems, you start to say, *The system itself is not just the software; it is the data that's being ingested and used within the software, and it is the evolution of the*

capabilities both innately in the software as it is. I'm not even going to say artificial intelligence yet. This is just modified systems.

Matthew: Sure.

Tom: And systems that are adaptive. We have adaptive in development. We have adaptive in the execution of these systems, and then we have adaptive in the deployment of these systems. Every one of those allows the flexibility for us to meet the moment and to be ready to meet the moment wherever we happen to be. It isn't just about agile software development. I think this is some of the misconception that people have. People think if we go to agile and we go to DevSecOps and we go to that, that is all we need. In fact, no, the agility goes all the way through the thread from the original definition to the deployment and the entire lifecycle of the system.

Matthew: I know you said your job isn't making predictions or forecasts, but it is really interesting to see that things that the SEI said almost 20 years ago have come to be the reality that we are living in now. You touched on AI.

Tom: Yes.

Matthew: I would like to explore that in a little more detail if we could. You mentioned the system including data.

Tom: Yes.

Matthew: This is a departure from the way we used to think about this, where data was something that was ingested or maybe produced by a software system. But now, what I heard you say, Tom, is that we really can't separate those things. The software and the data are all part of a unified system, which seems to me would need to modify the way we think about a number of things.

Tom: When we put a real system together, what we are doing is we are taking the software, and we are taking the data that is part of the system, and we are linking it to an entire sensor-based system around the software to ways in which the software and the data interact with the real world. This might be object detection through sensors. It might just be telemetry. It might just be various kinds of radar systems and various kinds of elements that sense our environment. But because the environment is changing, and because the environment adapts to where things are happening, the software is getting feeds of information into the system that are a part of

how the system has to operate. They are part of the capabilities that are being created in the system. It isn't just that we have artificial intelligence, right? We can talk more about AI and the infusion of AI into everything, but the way I like to think about it is that systems have gone from thinking about the Internet of Things and to thinking about control systems to thinking about every software system that way. Every software system has a link from reality through the data, through the software, through the behavior of what is happening.

Matthew: That is really interesting, Tom. It seems that these divisions that exist in the past have certainly blurred or eliminated now. From your perspective, what are a few priorities or research areas of top concern both for the SEI and for our DoD sponsor?

Tom: I think this is going to be a little interesting. I talk about being always ready for the next moment. Part of being ready for the next moment means that you want to structure our research not to necessarily solve today's problems, but to be ready for the problems that we have yet to anticipate. Now, I think about that as maturing the world of engineering. The future of software engineering incorporates research into what are the key quality attributes in artificial intelligence that are necessary for predictive creation of new software assets? What is the nature of cyber engineering to create trustworthy, predictable elements in the future of our software so that they are always capable, always ready to be used no matter how the moment changes? Our research is focused around expanding those areas of engineering. You would think we would be done with software. We've been doing it a long time, for 40 years. But in fact, the world of software engineering changes. We can even see that today, with regard to the software pathway with the DoD acquisition, within the idea of Secretary Hegseth's most recent memo on the use of the software pathway in all DoD acquisition of the future, recognizing that every system is a software-enabled system, and every system is going to need this coming into place. I look at all of those elements and think the role of the SEI and the research that we do, as we have always done, matures the area of engineering along all the quality attributes that are important to our future. That includes the overlap between artificial intelligence, cybersecurity, and software engineering.

Matthew: Yes, that is a great way to frame it. This convergence is really the most important facet of what we do that we should focus on. We are doing very important work in these disparate areas, but it is really that combination that is the most powerful. As an FFRDC [federally funded research and development center], one of the chief measures of our success is transition.

Tom: Yes.

Matthew: I was wondering, Tom, if you had thoughts about things that have been transitioned and maybe the nature of transition in this current environment.

Tom: The most important thing that we can do at the SEI is to change the nature of how the government and the private sector—federal government and the DoD and the private sector—change their behavior with regard to software, software engineering, cyber engineering, AI Engineering. Our transitions have largely been, how do we incorporate responsible AI into the development of AI-enabled software? How do we actually get analysis of the various kinds of static analysis techniques that we have for security into routine behavior for the software development in our systems? Not just something that you tack on at the end, but something that you bring into it. How do we actually get risk analysis to be a prime element of what we do, not just a report at the end? How do we actually get cost estimation in software to take advantage of all of the agility that we are now building into our software field factories and building into our acquisition? How do we get all of that to work together to create the future of quality attributes that we need to transition behavioral change in the acquisition universe, in the private sector, and in the response to problems that inevitably develop in software-enabled systems?

Matthew: I think we are uniquely positioned as an FFRDC in that we have a great deal of insights into what our mission partners in the DoD and the warfighter needs.

Tom: Right.

Matthew: …our work with private industry. I think it is safe to say we've seen a convergence in technology. The idea that the DoD is using only bespoke things is a deprecated concept.

Tom: For all intents gone.

Matthew: Right, exactly. I think about why this is so important to our mission where we can take the things that we know are most important in that commercial context and, perhaps reframing that, the way that DoD can best work with commercial entities and bring that to bear as part of our capabilities here at the FFRDC.

Tom: We have a variety of ways of doing analysis and looking at the risk and mitigating that risk throughout time. But you first have to recognize that what you are doing is a blend of commercially available software, bespoke software that is actually being created, and sort of that in-between world where you take some of the private-sector software that is out there and harden it and make it part of what is fit for use by the DoD. I don't know if that entirely gets to your question. But, in our working with the private sector, what we have always done is look at the very best techniques that they have produced and use that information with our knowledge of what we do for the DoD and for the federal government, and create this sort of magic-in-the-middle area, which takes the best of what's happening in the private sector and the best of what we know about the Department of Defense, and creates frameworks and behaviors and capabilities which can be used by both sides to create really robust software.

Matthew: I love this description of the magic in the middle. I know we are both very proud to work for an organization that has such a complete catalog of artifacts. For folks in the audience, Tom has mentioned a number of publications and capabilities. Those are available on our website in many cases. Certainly, I would encourage the audience to explore not only just the topics but the specific things we have produced as an institution over the last 40 years.

Tom: I will also make a plug…although I talk about behavioral changes, sometimes those changes happen through the creation of software that we have done. We have a very extensive GitHub that is a part of the SEI with a lot of released software. Sometimes that software is forked, and the behavior change says, *We have an approach here, fork this project in GitHub and create your own version of this with all of the capabilities that we have created and put out there in the public domain*. That is one way that we transition.
Matthew: Yes, so it goes from the magic in the middle to these derivative, additionally magical things that folks build based on the initial raw materials we provide, which is such an important element in transition.

Tom: That is right. Coming out in the very near future is our annual year in review. In there you will see all kinds of elements that we have transitioned into a variety of areas of the Department of Defense. In each one of those I would encourage the listeners here to say, look at these in a way not to just recognize that we transitioned to a lot of partners, which is great. But how can what we have done for some partners help you in the way that you are trying to create the future capability and be ready for that moment that we

cannot predict that is going to be happening in every sector of the private and public sector.

Matthew: Thanks, Tom. And that *Year in Review* publication will be available on our website for our listeners. Fantastic. Well, Tom, I'd like to thank you for joining me today to discuss this topic, and I look forward to where the future takes us as an institution and as your individual contributors here.

For our audience, the SEI Podcast Series is available in all the places where you can find podcasts: Apple Podcasts, SoundCloud, Spotify, and the SEI's YouTube channel. As always, if you have questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.