Zero Trust Architecture: Best Practices Observed in Industry

Featuring Matthew Nicolai and Nathaniel Jacob Richmond 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 Miller, and I am a principal researcher in the SEI Software Solutions Division. Today I am joined by my colleagues, Matthew Nicolai and Nathaniel Jacob Richmond, researchers in the SEI CERT Division. We are here to talk about a paper that they recently coauthored highlighting several best practices from industry that organizations can use in establishing a zero trust architecture, a topic we have talked about before.

Welcome Matthew and Nathaniel.

Matthew Nicolai: Thank you.

Nathaniel Jacob Richmond: Thank you.

Suzanne: I am going to call you Matt and Nate if that is okay.

Matt: That works.

Suzanne: Very good. We have audience members who aren't familiar with you, especially Nate, this is your first podcast with this. Could you tell us what brought you here to the SEI and the work that you do here? What makes it cool to work here at the SEI? Nate, let's go ahead and start with you.

Nate: Sure. I came here to research and work on improving cybersecurity operations, security operation centers, CERTs [computer emergency response teams], to work with our world-class CERT Division. My original background is in cybersecurity operations and incident response. As I have worked here, I have focused more on security architecture, the things related to improving cybersecurity operations. I think the best part of my job here really is the opportunity to work with a lot of different people and organizations, really, across the country and across the world to help implement solutions and accomplish their missions and goals.

Suzanne: Yes, we get to talk to people you wouldn't normally get to talk to in a corporate setting for sure. Matt, tell us a little bit about yourself, for those that haven't met you before. What do you think is cool about working here?

Matt: Sure. So again, my name is Matt Nicolai. I am currently a graduate student at Carnegie Mellon, where I'm studying Information Security Policy and Management. I have been here at CERT working as a research assistant now for a little bit more than a year. The majority of my research is focused on zero trust architecture and related topics. Among everything that I enjoy about my job, I would say that the standout thing is that I am surrounded by truly brilliant and kind people. I get to work with these people to solve novel problems every day. Every time I walk into a room, I am bound to learn something. I would say that is the biggest takeaway from it.

Suzanne: One of the reasons I do podcasts is I learn something every time I interview smart people like you guys. The learning environment here is something that I really appreciate, as well. To get to our topic, we have a number of resources, because we have talked about this before, that give people a good introduction to zero trust architecture, and we will include links to those resources in our transcript as we always do. But just so people have continuity within this podcast, can you start by giving just a little overview of what you mean by the term zero trust architecture, just so everybody is on the same page? I am not sure who wants to take that one. You choose.

Matt: I can go ahead. The zero trust architecture, kind of simplifying it, it represents a shift away from the perimeter or castle-and-moat style of network security that is ubiquitous today. In a castle-and-moat network, your network perimeter pretty much is the moat that will keep untrusted malicious actors from gaining entry. Meanwhile, the people who are inside the castle are trusted by default and can roam around relatively freely. Zero trust, one major element of it is that it removes that element of implicit trust from the castle-and-moat model. So we are going to constantly verify users' identities, whether they are inside or outside the network. Zero trust architecture is also characterized by the presence of a policy decision point, which you can compare to the control tower of an airport, where the tower is constantly looking to identify and grant access to aircraft. Much like zero trust architecture, they rely on internal and external intelligence, such as radar and CCTV [closed circuit television] at the airport to help inform their decision-making.

Suzanne: So no more castle and moat. Everybody is a potential spy, and everybody is a potential participant in what we are doing. Everybody could be one or the other, and we are not going to make any more assumptions about it. I think that is really, for me, the takeaway on zero trust is, we no longer make assumptions about who is trustworthy and who is not. We are constantly verifying that. In today's world, it makes sense. What are the challenges that organizations face in adopting a zero trust architecture?

Nate: I think one of the obvious ones that we see all the time is complexity. You know, the logistics, adjusting business processes, how things just work, and even just figuring out where do we start with this? Because it is really a journey. It is not a process that is necessarily just going to end. You will always be… As you bring on board new systems or your business changes, zero trust will also mean things might change to how you would have done that in the past. It is certainly complex. That is one of the biggest things, the biggest hurdles, and then also just resources, particularly expertise, like getting your people up to speed is definitely one of the factors there as well. I think those are the ones that always immediately jump out to me. When I talk to people about zero trust, it is apparent that it is intimidating because of the complexity involved in shifting a whole organization to zero trust.

Suzanne: The other thing that I would imagine is a challenge is the inherent complexity of this. But there is also… In organizations that have lots of people, hundreds of people, you are trying to make this as what I call *apparently simple* as possible. You are not trying to load that complexity on your end users. You are trying to shield them from as much of the

complexity as possible. So that has got to be a challenge, as well. Did you want to comment on that one?

Nate: That is certainly the case. Actually, I have the feeling that for most end users, when you get through some of this process, it actually becomes much more seamless, and security is easier from their perspective because you are moving away from things like VPNs where you have to log into this VPN to get access to like, say, your email, or your file storage, or all those things. In this case, it is mostly seamless. Every once in a while you, for example, maybe have to, you know, enter a multifactor authentication PIN or something like that to refresh your credentials, but otherwise, it is much more seamless. In some ways, it makes it easier for users, because they are not getting so many pop-up standard credentials all the time.

Suzanne: As a user, I applaud that. I just want to say. That is, I think, one of the things we want to emphasize is that just because it is complex in implementation doesn't mean that that complexity is going to actually get sent out to the user. People like me don't need to be afraid of it. Now, recently, you hosted a workshop on zero trust architecture. You invited industry professionals. That became the catalyst for the paper that we are talking about outlining what are the best practices in the industry. So tell us about the workshop, and why did you feel it was important to bring industry professionals to the table?

Matt: Sure, so SEI's Zero Trust Industry Day, it helped with bridging the gap between zero trust concepts and real-world implementation. In regards to the differences between public-sector and private-sector organizations, I think it is important for us to mention that the government's zero trust efforts are largely driven by executive orders on the regulations. Private-sector organizations are exploring zero trust because they are looking to adopt it as a best practice. As a result of that, they have very different considerations and priorities regarding this subject, but they can still find middle ground on things, and both had major takeaways from Zero Trust Industry Day.

Suzanne: You talked about differences between industry and government. What are some of the things that actually are the same that you found that might have been surprising? It is like, *Oh, I didn't realize that industry thinks about this the same way that government does*.

Matt: If you are going to look at zero trust and key tenets of it, they are the same, regardless of where you are at. Both government organizations and

private-sector organizations are mindful about resources, like minimizing costs and expenditures. If you are a publicly traded organization, like all this factors into your financials, and for government agencies, too, like sometimes they are resource constrained. We try to focus on discussing how to do more with less and repurpose existing tools and solutions and things that they might have and make smart purchases when they actually need to perform acquisition.

Nick: Just to add to what Matt said many of the participants in our [Zero Trust] Industry Day also have government customers. They are not just marketing their products or services to private industry. They also have government customers. So they very much have some incentives to keep both types of customers happy, to find that middle ground themselves, to make sure they bring solutions that are useful but also cost-effective, or at least competitive with older solutions. That was pretty interesting to me that they, as Matt said, on the government side, a lot of it is top-down from the executive branch saying, *Hey, you must do it this way*. But industry does take cues from that because they know they can increase their customer base by also paying attention to things like that.

Suzanne: OK. So, in the white paper, you outlined five best practices and how they can empower an organization's zero trust architecture. First of all, let's list what those practices are, and then I would like you to choose a couple of them to focus on that may be of interest to our audience. Just to say ahead, that all of them are elaborated in your white paper. Even if you don't pick somebody's favorite, it is still going to be in the white paper. So Nate, Matt, who wants to go on that one?

Matt: I can list them out if you would like, and we can take it from there.

Suzanne: Sure.

Matt: The first best practice we identified is inventories—the importance of developing and maintaining a comprehensive inventory that focuses on DAAS, so data, applications, assets, and services. As a subcategory to that is, you'd like to figure out, what are your high-value assets?

The second best practice is focused on auditing and logging. These are absolutely critical best practices to keep in mind when you consider the dynamic nature of zero trust and some of the challenges that may arise in the long run with the zero trust implementation.

The third best practice we were focusing on is governance and risk. That is because zero trust is a complex paradigm that involves a relatively long journey from introduction to maturity. Organizations we believe should leverage governance in risk management to help them plan, implement, and support their zero trust journey.

The fourth best practice that we have enumerated here is cloud and virtual solutions, where we think that these should be leveraged whenever they can reasonably fit into an organization's zero trust journey to decrease overall risk and help with complexity. The fifth best practice, the final one, is focused on utilizing automation, orchestration, and APIs to optimize maturity levels.

Suzanne: All right. Those cover a wide gamut of things, everything from governance to very detailed things like auditing and logging. Can you pull a couple of those out and give us some elaboration of, *What do you really mean by that best practice? What are some of the takeaways that you want people to have in relationship to how they might best do that practice based on what you learned in the workshop?*

Nate: Yes. I'll start with the first one. You mentioned the inventories. The interesting thing I think we mentioned a little earlier. Some of these things, or a lot of these things, are practices organizations do already, and inventories is one of those. But the difference is that to actually make this zero trust journey, you have to have the baseline… Particularly for the aspects you are focusing on, if you pick a specific area of your business where you want to make that zero trust journey, that is where you really have to make sure all your data applications, assets, and services are properly enumerated. In fact, it is so important that the industry participants in our [Zero Trust] Industry Day have mentioned a lot of their tools that are geared towards the zero trust journey include options that will help inventory as you are making that journey. For example, trying to automatically tag data as sensitive or just automatically tagging data or to help organize it as part of your inventory, and then, more properly move forward on the journey, so that you are using correct information to do so. I don't know, Matt, if you want to add to that one.

Matt: I think the other one that really stood out to us was focused on governance and risk. That was something that was emphasized by both the solution vendors as well as the government security leaders that we spoke to. Because at the end of the day, proper planning and logistical considerations are essential to zero trust success in the long run. I cannot emphasize this enough: zero trust, it must be maintained in the long run. You

don't just get there and you are done. You need to sustain this as part of your operations. Setting up a solid foundation up front to ensure longevity of your program is extremely important. Organizations can work towards that by creating roadmaps, investing in their personnel for transformation as well as operation, and focusing on straightforward approaches as they leverage their existing resources.

Suzanne: I think what you are really talking about here is keeping track of what is it that we need? The governance aspect that is important here is, is this still important data? Has our world changed, and now this data is not important, but that data is important? Understanding your business and operational environment, so that you can make good decisions about risk and make good decisions about where you are going to focus your resources. When you start doing these inventories, I know some people that have done some of this. They are amazed themselves. Even the IT people that sort of run the operation are like, *Wow, I hadn't really thought that we had that much stuff*, and that many services. Oh, my gosh. It can be overwhelming. That is really where a governance structure and a governance framework can help you is in sort of saying, *OK, this is the important stuff. This is not as important. We can move forward on the important stuff first and really get somewhere*. That is kind of what I got from the paper in terms of what your real focus on governance is.

Nate: Yes, absolutely. I agree with that. To add to it, if you look at it, I can barely keep track of all the devices on my home network with the various things. When you think about a true enterprise, you are absolutely right. None really have a completely accurate inventory because not only is it tough to find everything, but things constantly change. Things are going off and on the network and all sorts of things like that. That sort of ties into this governance discussion because at some point you have to just say in a zero trust journey, *All right, let's start. Let's just pick something and work on that*. And a lot of people will even say, *Oh, but what do we pick? Where do we start?* There are recommendations and guidelines, like, pick something you know well, like a service or a business, some part of your business you know very well to tackle first or a small, manageable chunk. But ultimately, you just pick something. Don't try to get caught up trying to pick the perfect thing, and then perform that governance to really understand where you are going and readjust as needed when things inevitably don't go exactly as planned, because it is still IT. It is not going to go perfectly.

Suzanne: Is this a case where perfection is the enemy of the good? You know, so we can get some good results without being perfect. We want to

strive for perfection eventually, but as you say, *I may not be able to inventory everything across the whole operation, but I can inventory this important area of my busines, and we can start to govern it and start to bring the tools in to take this piece of it and make it better*. Is that a fair statement to make?

Nate: I think so, at least to some degree. Certain things, maybe you have less room for error or not being perfect. But yes, overall, certainly with the zero trust journey, you shouldn't expect everything to go perfectly or have perfect plans. Just like any project, and especially a big one, it is not necessarily straightforward. Which is why we have something like this with the best practices where we try to break it up into manageable chunks to make it a little more approachable or easier to think about.

Suzanne: One of the things you have done by doing this is actually going into sort of our next topic, which is transition. Helping people to focus is one of the aspects of transition to sort of take that whole big landscape and say, *OK, if you just look over here for a little while, we can get somewhere*. What are some things our audience members can take away as things that the SEI is providing, and/or things that are out in the public domain that they can go to, to help them with transitioning to a zero trust architecture? At this point, it is no longer kind of a new phrase. I mean, we've been hearing it for several years now. So what are some of your favorites in terms of resources that newbies to this idea could actually use?

Matt: Well, the first is a shameless plug for our previous white papers.

Suzanne: I said SEI, so I will allow it.

Matt: We have tried to break down the transformation process into, I guess, more manageable chunks and very simple, easy-to-understand terms. When you read some of the standards and stuff, they are good, but there is that gap between like what the concept is and what it is going to actually look like in practice.

Suzanne: Exactly.

Matt: That is the approach that we took with developing these best practices here because we tried to address potential pain points that were raised by both solutions vendors, as well as leadership in regards to previous transformation efforts and now going into zero trust. In regards to resources that are out there that I would say are worth exploring. One of them that stands out is NIST [National Institute of Standards and Technology] has

recently pushed out *Implementing a Zero Trust Architecture*, which is, I think it is a five-appendix, five-series implementation guide about how organizations can utilize existing resources and available solutions out there to try to implement zero trust in a manner that aligns with the NIST standard. They utilize tools, and they document it pretty much like how you can set up, for example, things like a Zscaler to work in alignment with what they have in mind, for zero trust. I think that is one that more people ought to explore.

Suzanne: OK, anything on your radar, Nate, in terms of favorite resources for people that are new to adopting zero trust?

Nate: Well, I think Matt mainly mentioned them. I think, right now, many of the resources are civilian government resources, but there are also industry players that we mentioned in our blog post and paper that have resources, as well as documentation, about how do you start on this that are also useful. We definitely don't want to ignore industry's experience because they have to actually go into some of these government agencies and their other customers and help them implement this stuff. They have some good visibility into what people struggle with and what they do well with.

Suzanne: For both of you, what is next? You have got five practices? Are we looking at being done when you have 10? Are you doing some other things? What are the things that you are working on in terms of… Matt, you have got some educational goals I know you have got to deal with as well as your CERT goals. Nate, I know, cybersecurity operations is a big, big, big pool to play in. What is going on with you guys? What comes next? Matt, start.

Matt: Sure. On the educational side, I am currently working on my graduate thesis, which is focused on governance and risk.

Suzanne: How about that? I didn't know that. He did not prompt me with that. I just want people to know.

Matt: Yes, it is in the pipeline. On the zero trust side of the house, we are soliciting feedback based on existing works and trying to identify what subjects does our audience want us to go deeper into. We put out resources, and there are other agencies, government organizations, private-sector groups, et cetera, that are pushing out resources. We try to address gaps in what is out there and help people navigate the lay of the land. We are keeping an eye on existing feedback, and we are working on putting together future events to bring government and the private sector together again to work toward zero trust implementation.

Suzanne: Excellent. We will look forward to some blog posts on that in the future then. Nate, what are you looking at working on?

Nate: Well, in addition to the zero trust topic, we have been doing some work on acquisition and security, plus just helping cybersecurity operations teams shift with the change to zero trust because it does mean different, for example, perhaps, data feeds coming in that you use for your analysis and things on along those lines. Not only just how they adjust their processes, but what do they really want to get from it. If it is really changing how the network looks, then you have to also change how you are doing that analysis when you are doing, for example, incident detection and response.

Suzanne: OK, I hadn't really thought about that connection. But yes, if you are looking at different data coming in, that is going to affect some of your analysis techniques and some of your results. You don't want to be having false positives when you don't have to.

OK, so, Matt and Nate, thank you for talking with us today. We are going to include links, as we said earlier, in the transcript of all the resources we have talked about, and I'm sure some others, including your white paper and your blog post. To our audience, I want to remind you that our podcasts are available in lots of different places, Stitcher, SoundCloud, Apple, Google, and of course our favorite, the SEI YouTube channel. If you like what you see and hear, feel free to give us a thumbs up. Thank you both again for joining us and to our audience, as well.

Matt: Thank you for having us.

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.