Carnegie Mellon University
Software Engineering Institute

SEI Podcasts

Conversations in Artificial Intelligence,
Cybersecurity, and Software Engineering

Orchestrating the Chaos: Protecting Wireless Networks from Cyber Attacks

Featuring Joe McIlvenny as Interviewed by Mike Winter

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.

Mike Winter: From early 2022 through late 2024, a threat actor, publicly known as APT28, exploited a known Windows print spooler privilege escalation vulnerability to remotely and wirelessly access sensitive information from a targeted company network. APT28 executed the attack by compromising less secure Wi-Fi networks of multiple organizations that were in close proximity to the intended target. The attack did not require any hardware to be placed in the vicinity of the target company's network. It was executed remotely from thousands of miles away and used system-level privilege exploitation to install backdoor access and steal credentials. This incident brings to light the critical role that software plays in the security of modern-day wireless communication systems, both in the military and civilian realms. Welcome to the SEI Podcast Series. My name is Mike Winter, and I am a vulnerability analysis technical manager for the SEI CERT Division. Today, I am joined by Joe McIlvenny, a senior research scientist also in CERT. Today, we are here to talk about this emerging threat landscape of wireless attacks and efforts underway here at SEI to address them. Welcome, Joe.

Joe McIlvenny: Thank you.

Mike: This is the first SEI podcast for both of us. Let's start by telling our audience about ourselves, what brought us to the SEI and the work we do here. So, Joe, let's start with you.

Joe: Sure. Absolutely. Thanks. I have a background and education in computational physics. I did my undergrad in computation physics, and then I have a master's in applied physics. Out of school, I worked for a contractor for NOAA [National Oceanic and Atmospheric Administration]. This was my first exposure. I worked in the satellite department there, script slinging, essentially writing scripts that take the satellite data, process it, working with the scientists there that write the models for the codes, for the weather things, the weather models. This was sort of my first exposure to wireless and RF [radio frequency] comms, remote sensing, and it was pretty cool. And from there I worked at the Johns Hopkins Applied Physics Lab down in Maryland. There I worked with some really great people over the years doing all kinds of things from designing and building sensor systems, magnetic field sensors, quantum sensors, things like that, and also wireless RF sensors. About half of the time I was there, I was in the communications branch. What brought me to the SEI is, as I was working in the wireless branch there, helping design systems for users, customers, the military, and doing test and evaluation of those, you start to see things that… security issues or things that can be exploited. What really drew me to the SEI then is this kind of new area of, as you have this world of wireless technology, wireless communication systems and RF and this world of cybersecurity, cyber ops. As we move towards a more wireless world, those two things are really starting to converge, right? The ubiquity of wireless sensors, it is everywhere. It is a growing concern I think and should be for folks that have communication systems that overlap with cybersecurity systems.

Mike: That is incredibly impressive, Joe. That is not going to be a fun one to follow up, I would invite our listeners right now, if you are going to have a chance to let your mind wander, it is probably my turn listening, hearing what I did as a background. This is not going to be fun to follow up. My background is in the military. I was in the Air Force for 24 years. I started off in special operations. From there, I went into intelligence primarily where I worked in national and tactical intelligence operations. Then, the third half of my career, was primarily in cyber operations in support of cyber command. Not with the extensive background that you have in RF [radio frequency] and physics and all those other things, so I appreciate that. Thanks, Joe.

I joined the SEI primarily because the SEI has that reputation of having that objective highly specialized, long-term research and development and analysis that is definitely needed across all walks of the department. I really have always been interested in AI solutions in terms of the high-ops tempos and things like that you have in the Department of Defense. I always found that to be a very fascinating topic to try to help out our soldiers, sailors, airmen and Marines and a lot of what they do day to day. That is what brought me to the SEI. I work in the vulnerability analysis team, and we specialize in vulnerabilities. Vulnerabilities exist everywhere. What are we going to do about it? It is kind of a challenge. With that, I am going to open with a very important question. I think first and foremost, our listeners want to know, Joe, what is your walk-up song when you enter the office for a meeting, or you just enter the office in general, you come through those doors of SEI.

Joe: That is a good question. I am a metal head at heart. I have always been a heavy metal fan. That is a tough one. I think anything from the first four Black Sabbath albums are a given, right? Always classic. There are some good…When you need a more of a pump up, something faster. I have also always been a fan of thrash, so thrash metal like some good old Metallica or Megadeth. It depends on the day and what is on the list. What about you?

Mike: I like it Joe. I was doing a little mind reading and my mind reading was off. I was thinking you were into Barbie, Barbie world.

Joe: But some days it depends on the day. You never know.

Mike: Mine would absolutely be Led Zeppelin's Kashmir. It is cinematic. It is very confident. I feel like I am wearing a cape when I hear that song. That just makes me think when I walk through the doors of SEI that is my go to. Last question before we dive into the actual podcast here, considering that we are going on a podcast journey together, who is the better singer Steve Perry or Arnel Pineda?

Joe: I mean, Steve Perry, right? No one can sing it. No one can make you feel what does a broken heart feel like Steve Perry. He is a classic.

Mike: Steve Perry's probably not listening to this podcast, but if he does someday, he'd be very proud, so thank you.

All right, let's spelunk into wireless attacks. A report from the office of the

Director of Operational Test and Evaluation stated that our nation's cyber posture remains at risk from attacks by unconventional threats such as those posed by radio frequency enabled cyber attacks where cyber payloads and radio emissions disrupt systems, or direct attacks on weapons systems, data busses, and control systems that are central to aircraft, ships, and vehicles. That is a long sentence. The APT28 attack discussed in the introduction is an example of a targeted attack demonstrating the ability to sidestep MFA devices. What other types of attacks are we seeing in the field right now?

Joe: Yes, that is a great question. Just to elaborate on the APT28 attack a little bit, that nearest neighbor attack was a really unique and creative way to get at information that they were trying to get. They attempted to do a password spray and gain credentials from their targeted company, but they found that they couldn't get into the system because they had multi-factor authentication things, so your YubiKey or Duo on your phone: things that require multi-authentication things instead of just a password. What they did was then they targeted organizations that were in close physical proximity to the target. They found that those organizations had less secure Wi-Fi. They had what was called a multi-home Wi-Fi. What that means is it has an ethernet connection and a wireless connection. They were able to get into those Wi-Fis and then use that to access the target company's Wi-Fi. What they found was that while the network in the system had multi-factor authentication, the Wi-Fi was not protected by multi-factor authentication, MFA. What they did was now that they had the passwords that they had got in a separate campaign, they used the near-proximity organizations to get into the target organization to steal the data and the information that they were looking for. To do that, they exploit it as you mentioned at the beginning, there is a print-spool privilege vulnerability. We have the number here somewhere. We will put the link to it in the podcast transcripts.

But that vulnerability allows someone to…In the print spooler it uses JavaScript essentially to help with the layout of when you send a print job to the printer from your computer. What it does is it allows system-level access to the user. By exploiting this vulnerability, they were able to escalate their privileges and capabilities to system level so that they could go in and insert malicious code to steal, to give them a backdoor, like you said, to be able to steal the information, to steal credentials, to get in. Again, what is really interesting about that particular attack is that they didn't need anybody or any devices in the area. They did this attack completely remotely from the other side of the globe and didn't require anyone to be here by the organization. A little disconcerting, a little concerning.

Mike: There is a level of sophistication there too and a level of persistence by the adversary. It is easy to look the other way and wish it away, but that is the adversary that is on our doorstep. If they want in, they are going to find a way to get in.

Joe: That's right.

Mike: It sounds like the RF is a pathway that is exploitable, and we might have some openings there.

Joe: Right. Some other examples, of course there is the typhoon APT [advanced persistent threat], and they are always in our infrastructure. There has been reports about that out there. What they do, they really look at exploiting industrial SCADA systems, the Wi-Fi in industrial SCADA. They will insert like rogue access points in the vicinity of a target. So that gives them, again, exploiting Wi-Fi vulnerabilities or a lack of multi-factor authentication on the Wi-Fi to be able to get into a network by hopping across Wi-Fi connections, access points. They often have compromised Internet-of-Things [IoT] devices. If you think of IoT things, they are everywhere, right? Bluetooth, speakers, headphones, watches, your refrigerator. Everything is somehow connected.

Mike: I think if you and I were texting right now, you would be getting a lot of surprise face emojis from me and a bunch of grimacing face emojis from me right now, because that does not sound like a healthy place to be. Here is kind of a fun question for you, if you had a fantasy draft of cybersecurity practices, given what we just talked about, what would you pick in the first round given what you just said?

Joe: Oh man, that is a good question. I think again, it is hard, right? There are so many ways to be able to protect the system, but there is always a loophole like we just talked about. But I think doing things like ensuring that your software patches are up to date, that is always important, and NIST provides guidance [see here and here] on how to do that and lots of others too. Having things like the traditional things that we talk about, strong passwords and not just *1, 2, 3, 4, 5*, and other things like that. Another thing that we talk about at least at the enterprise level is having role-based privileges. If you are logging into the system, you can only do so many things based on the role. Whether you are an administrator or you are just a normal user or you are a visitor, each role has a different set of things that they should be allowed to do, a different set of privileges within the system and having guardrails around like not being able to skip across those. Like I log in, and I say, *sudo do whatever*, so things like that.

Mike: Yes. How have software and cybersecurity played key roles in these exploitations. We have covered a couple of them right now, but let's hone in a little bit more on that one right there. Where exactly have those software in cybersecurity played key roles in those exploitations.

Joe: Yes. Looking across the OSI stack at all of the layers, there are exploitations and vulnerabilities at each layer. Just to do a comparison between some of the traditional wired system versus a wireless system. When we talk about security in a wired system, we usually talk about confidentiality. That is ensuring sensitive info is only accessible to authorized users, and it can't be intercepted or unintentionally disclosed to unauthorized users, so confidentiality. And then integrity, that is a guarantee that the data remains accurate and unaltered. That is to prevent unauthorized modifications or corruption to the data. Then, again, in wired systems, the third one is usually availability. *Is that data available to the authorized users when they want it, when they need it*?

In contrast with the wireless-type systems, security in wireless systems, those things all apply, right too, but what we usually talk about in wireless systems is *covertness* and *robustness*. What *covertness* is, that is your measure of difficulty. *How hard is it for an eavesdropper to identify the existence of your link?* That is detection, right? And what is the measure of difficulty for them to intercept data to extract data from the wireless link that you have. That is *interception*. And then *robustness* is the measure of how difficult it is for an attacker to disrupt the link. Think like anti-jamming or jam resistance that sort of thing. What is different in both places from a security and a data perspective? Both networks need channel coding. Both networks need signal processing, but the fundamental approaches are different. For example, in a wired system, you have a wired gigabit ethernet connection. The quality of the copper wire in the winding adapts how the channel coding is done and the signal processing on the network. The most reasonable way to intercept data in that situation is a wiretap. You have to have physical access to the wire to be able to extract that data. In contrast, on a wireless system, the channel coding and the signal processing are potentially public because you are broadcasting over the air and just because of the wireless nature of the links and the connections. The implementations need to have the robustness incorporated into that design, because it is certainly much easier for someone to intercept a wireless signal than it is to find the wire and tap it. That is part of what makes the security of wireless systems harder. You can say, *Well, we have it encrypted. Our signal is encrypted*. *It is fine because we are* *encrypted.* That gives you a level of security. But there are a whole set of things that you can gather below the encryption layer in the OSI stack at the physical layer. I can see what frequency you are broadcasting on potentially. If I am sophisticated enough, I can capture your hopping rates: how frequently or quickly are you changing frequencies to try and obscure things? I can do a pattern-of-life assessment, like what time of day do you broadcast? How often do you broadcast? You can do things like triangulation if you have sensors up and around, where is your location? All of those things are potential vulnerabilities that can be captured below the encryption layer. That is not withstanding vulnerabilities in encryption implementations and stuff too.

Mike: For those of you who don't know Joe, I think we all sort of understand him better, especially through his walk in song. Because I can understand why you listen to thrashing metal every day as you walk into the office. I think I would too if that is the matrix that I see every day all around me. With that, let's ask you a fun question. We will just lighten it up a little bit here as we move on to the harder ones. Would you rather be forced to use public Wi-Fi for a month or run the default passwords for a week?

Joe: Oh man. Boy, that is tough. Probably, oh man. I would rather do neither given the choice. I guess public Wi-Fi as long as you have the guardrails up to protect yourself. Things like, I have secure passwords. I can monitor the system to know if there are people trying to gather my information. And you can put sensors up to do that, an SDR with a receiver looking for anomalies and rogue signals.

Mike: Yes. I'm not so sure if I want to trust that wheel in the sky, but I will probably just write a letter. All right, all right.

Joe: Fair enough

Mike: Back to more serious questions here. Joe, the next question is, the ODT&E report that we referenced earlier, went on to state that future cyber strategies, resource allocation, development, and testing must consider such cyber threats. What efforts are underway here at the Software Engineering Institute on this front?

Joe: Yes, that is a great question. Certainly, we have a lot of things going on. Looking at it from just a cybersecurity standpoint, we have a plethora of experts here that know how to really dig into systems and understand the vulnerabilities of them. And taking that expertise and trying to apply it to wireless systems is a lot of what we do. Like we talked about, that is my background, and that is why I am here. We have a laboratory set up here on campus, th at is looking at the [IEEE] 802.15.4-2020 standard. That is where we started. That IEEE standard is the basis for a lot of mesh-network-type things. So, think of your internet of things. Those all sit on 802.15.4 and Wi-Fi and Bluetooth to some degree too. But things like Internet of Things protocols and waveforms, Zigbee, Wi-SUN [Wireless Smart Utility Network], those types of things. What we are looking at is, there is some level of inherent chaos in the network when you set up all these nodes, and they are talking to each other, and nodes are coming on and off of the network. What we are looking at is, are there vulnerabilities that we can exploit either at the physical layer below encryption or at some of the higher layers in the network layer, of the OSI stack, where some of the routing happens for a mesh network example. At least in Zigbee, it is handled at the network layer. What we are looking at is how can you understand what is going on and affect the network in some way to say like, *Oh yes, that thing happened, and how can we make the network more robus*t? Like we went back to talking about just the reliability. *Can we intercept it? Can we get data from it? How can we affect it? Can we take nodes down and have the network get confused? How does it reconfigure? What is the sort of latency in the messages when that sort of thing happens*? By being able to understand those things and mitigate against them, we can help to have a deeper understanding of how we can implement things in software to help the security of more important networks than just publicly available ones. Along those lines, it is an exciting field to be in right now, and it is exciting to look at. As we move closer and closer to the ubiquity of wireless signals, they are everywhere, right? You sit down at your desk, and you are on the Wi-Fi now because we don't normally plug into ethernet anymore. You have got a wireless mouse that is Bluetooth. You have got your wireless headphones for your Zoom calls or whatever. You have got your phone probably sitting on the desk beside you that is connected to.

Mike: Or behind me.

Joe: Or behind me. Yes. Wherever. But all of those are different compared to 15, 20 years ago when everything was still wired. It doesn't make it less secure. It just makes it concerning that we have to understand those vulnerabilities and where they exist.

Mike: Yes. The thing I want to build on is especially for the listeners and—especially you, Steve Perry, if this is the first time you listen to this podcast—what Joe just described there is all the wonderful things that people at the SEI are doing. I will give a little bit of a different perspective. As a listener, you can't really see what these folks are doing, but I can explain exactly what our teammates, what is inspiring them. People do not join the SEI to hide. They don't join the SEI to cower or to play it safe. You are coming here because there is something that is calling you and telling you you need to do something about it. You need to serve the public interest. You have an objective idea about something, and you are willing to go that extra mile. This is the vehicle to use. This is an FFRDC. This is why we come here. We are just surrounded by these exceptional people building out the horizons and the pathways of the future. Other things that Joe was kind of covering was the collaborative partnerships that we have, whether it is domestic or internationally, across academia, government, industry, it doesn't really matter. We are willing to do whatever it takes to basically provide that future state that we need to be in to serve the public. It is such an exceptional place to be. A lot of the things that Joe just highlighted are examples of the wonderful things that people do here to serve the community going forward. One kind of fun question before I get to my next question is what is a cybersecurity hill are you willing to charge with a fully loaded laptop, one that you are not going to stop believing? Out of all those wonderful things, what would you put up at the top like, *Man, this is one I am willing to charge that hill with my laptop*.

Joe: That is good question, too. Yes. Again like I said, just finding ways to make wireless more secure. It is a crazy time in the world right now and helping people, not only just the military, but helping folks to just to understand and raise that awareness of like, there are a lot of bad actors out there. We have highlighted some of them here today, but there are more. Just raise awareness. Let people know that my cell phone is a tool that just lets me do whatever I want. There are so many things in today's world…It is a super powerful computer in your hand, and it is connected to everything, right? Wi-Fi and cellular networks and Bluetooth and everything. Help people understand that it is meant to do all of those things, and you should absolutely use it to do all of those things, but do it smartly. Understand that, yes, there is a reason why we say don't use, *1, 2, 3, 4, 5* as your password. Yes, it is easy to remember, but it is also easy for people to crack.

Mike: Great Spaceballs reference. Yes. Alot of what I learned from Joe to all the listeners, a lot of it has to do too, with like, it is very easy to think about cybersecurity and think of it from, like a device. But we oftentimes forget the RF [radio frequency] side of it, and they are not going their separate ways. They are converged completely and going in the exact same pathway together, which leads me into our next question here. As a federally funded research and development center, a core aspect of our work is transition, not just building something for us to look at and celebrate and walk away from. Transition is at the core of what we do as an FFRDC. What resources are available for organizations who want to secure their networks from wireless attacks, and what should their next steps be?

Joe: Yes, that is a great question too. You are absolutely right. Like you said, we are not here to hide. We are not here to like, do something cool and say like, *We did this. Good job*. We are here to help serve the public and the military and everything. You mentioned them all: academia, industry, the government, just the general public. I think just being aware of the resources that are out there. Hopefully we can help do that with this podcast and the things that we do and our blog posts. The SEI is very good at having things out there that try to help people understand the challenges. Between our Cyber Minutes, YouTube videos, these podcasts, our blogs, all of those things, the conferences that we attend, the interactions that we have. Just maintaining that reputation of the expertise that we have and how we can share it. I think next steps if you have questions, or you want to reach out to us. We have resources constantly. We are always happy to help. Again, as an FFRDC that is what we are here for. If you see our booth at a conference, come and ask questions. If you have a question, the blog posts and the transcript for this podcast will have links, resources that you can reach out and look at. We have the info@sei.cmu.edu email. There are ways to try and figure out like, *How can I make sure that my data is safe and the things that I am doing are intelligent from a security standpoint?*

Mike: Exactly. Well said Joe. SEI is that place where the little Venn diagrams of curiosity, service to each other and service to our country and just a desire to have a strategic outcome come together. Everything you have just described there just radiates that point right there. Joe, we are coming to the end of our podcast. I do have some closing fun questions for you. It is going to get really fun here.

Joe: All right. I am ready.

Mike: Before we get into those, what is next for you? What are you working on that we can bring back in a few months to discuss. I have a feeling our listeners are going to like this podcast, and they are going to ask for us overwhelmingly to come back and do another interview. For a Joe and Mike, interview part two, what are the things that you can highlight as just a foreshadow for our listeners?

Joe: That is a great question. One of the things that we are really looking at again, building on the things that I have talked about. That is expanding to more protocols, more waveforms, more standards outside of just 802.15.4 where we started.

Another thing that we are really looking at is radio frequency propagation models. One thing that I didn't really talk about in my intro is modeling and simulation, and I have done a lot of that too. For those of you that don't know, in the world of like, *I have a transmitter, and I have a receiver, can I get a message from here to here wirelessly?* We do what is called radio frequency propagation modeling. That looks at things like the propagation of the signals. How do they get from point A to point B or from point A to point B-through-Z sort of things or multi transmitters? It is a really complex and mathematical field. One of the challenges in modeling and simulation is the realism. You can write a model—and this is not just for RF, this is for any modeling and simulation. You can do a mathematical model, but you have to validate it with real-world collections. A lot of the models that were written to do things like propagation were written forever ago. They are really great. They are in Fortran, which is science-level code that is awesome for those types of things, but they are slow because they were written before things like parallelism and the modern computing platforms that we have now existed. One of the things that we are really looking at is how can we help to either parallelize that code or write algorithms as part of that code to help speed it up? The goal there to speed up the processing, the computation time, is to help push it to the edge. When we have someone in the field that is experiencing multiple interference transmitters, jammers, whatever, and it is affecting their mission in some way. How they do it now, is they will have a mission plan, and they will say, *OK, these are the frequencies you use. These are the comms you use*. *This is the power level*. *Go do.* You get in the field, and you experience interference and things that you don't expect. A lot of the warfighters are great at fixing that on the fly, but we don't have the resources to be able for them to say, *OK, let me recalculate real quickly. Because it is like, Well, that model takes 14 hours to run it*, and that is not an exaggeration, the way they do it. Yes, it and it works great, but at the edge it doesn't work. We are looking at ways at how we can help accelerate those things and working with folks in our AI department, the artificial intelligence department, who do things like creating machine-learning models to do signal identification. How can we push those to, smaller-form factor type things at the edge. Maybe we will come back and talk about that and bring someone else from the ACL to help, the Advanced Computing lab.

Mike: Sounds lovely. That would be amazing. I think multiple podcasts going forward. So what we are going to do is we are going to close with a couple questions to Joe. The reason I am doing this, OK, may be on the subject. It may not be, but I want to try to bring the listeners into, maybe if you were in the SEI walking around, you might hear one of these questions being asked to somebody in a hallway. Because we like to have fun, too, right? You want to come in, you want to make a difference, but at the same time you want to enjoy what you do. I have a couple of fun questions to ask Joe to kind of demonstrate some of the conversations we may actually have after this podcast.

Joe: All right.

Mike: The first one, Joe, what is a superpower you would like to have for one day whether it is professional or personal?

Joe: That is a great question. This takes me back to the college days when you are like, *If you could have any two X-Men powers, what would they b*e?

Mike: Exactly!

Joe: I was always a fan of Magneto's. By the way, my two are Magneto's and Wolverine's because there is metal everywhere, and the magnetic field is always around us. I sort of hinted at I have done a lot of magnetic-field-testing in my day too. Then very little can hurt you if you can control metal everywhere. Then, if you do get hurt, you have the fast healing of Wolverine.

Mike: Wow, that is a heck of a superpower.

Joe: What about you? You don't get off.

Mike: Yours was definitely a very intelligent answer. Mine was simple, just teleportation. I would love to get like a cup of tea in Madrid and then pop up in Tokyo for a few minutes and maybe just understand some culture there. I would probably just bounce around the world for 24 hours and just try to take in as much as I could.

Joe: There you go. That is a good one.

Mike: But I'm not controlling magnetic fields. I wouldn't know what to do if I could control a magnetic field. All right, so this is a fun one. What's a goal you have no business chasing, but you might just do it anyway.

Joe: That's a good one. I often. Yes. Hmmm.

Mike: I will let you off the hook for a second. I thought about this myself. Okay. As you think about it, I think I am going to dedicate myself to becoming the world's leading expert in office walk-up songs. I think it is a space that nobody has kind of conquered yet. I think it is wide open. I already have two. I have mine and yours. I think I can build upon that. That is probably going to be the aimless task that I am going to go for.

Joe: That is a good one. That is a good one. I think as we have hit on, I am also a music fan. I have tried a couple of times to compile a list of—and I know these lists exist—but what are the essential albums that you have to listen to before you die, right. And they span all genres, but what makes a good album I like to think about. When you listen to Ride the Lightning like it is all killer. No filler. There is not a bad song on that album, but what makes it that way. Where does that translate to an Elton John album that might be the same or whatever. Like you know that. It is a daunting task to listen to everything and then be able to assess.

Mike: I think we found a new space for that intersection between music and software engineering. I think this is something we can build upon here.

Joe: Yes.

Mike: OK, I'm going to ask one last question. If listeners were to remember one thing from this podcast and it is definitely not music, but one thing from everything that you have discussed here and shared with us, what would be that one thing you want us to you want those listeners to walk away with?

Joe: Yes, I think that one thing is that wireless signals are all around us. We use them every day. We have to understand the implications of that and make smart decisions or gather information, use the resources to make sure that we're doing things in a secure way so that our information is not shared, our personal information, our names, our passwords things that could be exploited. On some level, you can say, *I can hide in the noise of 50 million TikTok users, but what happens when it is not, right? What happens when it is you that is compromised?"*

Mike: I appreciate that, Joe. Great answer. It has been a privilege, doing this podcast with you today. I am just so proud that the listeners got a chance to actually hear from a true SEIer that is paving future pathways and things like that. It is incredibly inspiring to know that the best and brightest that I have ever met are here doing everything they can to serve the public interest. So, thank you for that, Joe. We have had a wonderful journey today. For our audience, as previously mentioned, we will include links in the transcript to resources mentioned in this podcast. Finally, a reminder to our audience that our podcasts are available everywhere you find podcasts, including the SEI's YouTube channel. If you liked what you saw and heard today, give it a thumbs up. And we definitely appreciate you joining us today. Thank you.

Joe: Thanks.