Trust in Paradise

Embedding security, data protection, and privacy into products to meet today's cybersecurity challenges.

Michelle Dennedy: The significant security vulnerabilities, Meltdown and Spectre, recently discovered in the world's most popular computer chips, have the potential of exposing millions of users to hackers – and to the theft of sensitive personal information. Secure Development Lifecycle or SDL, or "CSDL," as we call here at Cisco, is the process [that] technology companies use to ensure that their products are safe and secure.

What happened? How is secure development evolving to stay ahead of the bad guys in hardware, software, and in other types of services? Stick around as Ed Paradise, Cisco's Vice President of Trustworthy Systems Engineering, brings us up to speed, and along for the journey, his long-time companion and our first privacy engineer, Ms. Lisa Bobbitt.

Cybersecurity, data protection, privacy. You like to stay ahead of the curve and listen to experts who are leading the way in deriving greater value from data with a more organized approached to data privacy. You're like us, just a few deviations past the norm. You are a Privacy Sigma Rider.

Hi, all, it's Michelle Dennedy once again. Chief privacy officer and vice president here at Cisco. My guest today is Ed Paradise, vice president of Engineering in our Security and Trust Organization. As the leader of Cisco's Secure Development Lifecycle, Ed and his team of engineers and product marketers develop the tools, processes, and technologies we need to minimize threats to Cisco products and services, and to ensure they comply with our evolving standards for security, data protection and privacy. Ed, that's the formal marketer's rollup of you. Tell us a little bit more about your background and how you were trained, and how did you find yourself running these crazy cats and herding them as best you can?

Ed Paradise: It's a pretty simple task, and I'll be 25 years with Cisco in April all here out at the RTP campus.

Michelle Dennedy: Wow.

Ed Paradise: Back in the early days of Cisco, Frank Marshall was the VP of Engineering, and came to the conclusion that at the growth rate, we wanted to achieve that being a company only in the valley wasn't going to cut it, so he decided to open an office on the East Coast. Prior to that, I'd been working for IBM for a number of years, and we did a joint project with Cisco to show the world how we could take local area networks and connect them to mainframes. One thing led to another, and I was proud to be part of the initial team here that opened Cisco on the East Coast in 1993.

Michelle Dennedy: Wow. That's a long time. A quarter of a century of security. That's a lot.

Ed Paradise: It wasn't all security. In the beginning, it was about taking legacy networks and converting them over to the internet protocol. We did that with the IBM, SNA, big type customers. We did it with SS7 and service provider. We did it with voice and service provider, voice and the enterprise,

and then I spent a number of years in software quality, and then to the global government solutions group.

That's really where my roots in security really dug in because we worked with governments around the world to take Cisco's product portfolio and make it more relevant for them by putting in features that were available on all our products. We really never sold anything that was specific to the governments, but they gave us stringent requirements for what did they needed for encryption and other things, which led to the security and trust group, and that's how I and the engineering team progressed into this domain, and we're having a blast. There is no doubt of as we read in the newspapers. There's never a dull moment on the security front right now.

Michelle Dennedy: It's so true, and I want to tease out a couple of the things that I'm hearing, and then we'll have Ms. Bobbitt introduce herself too. First of all, RTP, when I first arrived at Cisco, everyone was saying that they were in RTP, and I thought it was some sort of a space pad. It's actually a research triangle park in North Carolina. It's a gorgeous, gorgeous part of the world, and it's really fun. We are a global company indeed, and there's always an interesting energy where the folks in North Carolina are getting their launch, and we're still probably on our second cup of coffee out here in California, so it's always fun, and Ed's there now, and I've dragged Lisa out here out west.

As we go along, I'm going to highlight these words that you've already used, and we'll throw them in our common conversation, which is conversion of legacy, this constant transition. 25 years ago, you're talking about transferring legacy, quality, the notion of, "What is quality in a rather ..." You have a limited tool set. How do you create quality out of what you've got and continue chasing that? Then, government solutions and the word solutions itself, and what does that mean to us today in a cloud-based, solution-based, services-based ongoing environment?

Before we dig into that big pile of goodness, Lisa Bobbitt, please reintroduce yourself. You've been on this show a couple of times, but I want to make sure all listeners are aware who my partner in anti-crime is.

Lisa Bobbitt: Hi, I'm Lisa Bobbitt. I am the Privacy Engineer here at Cisco. I'm working with Michelle, but I work with Ed for almost all the time I've been at Cisco, which was 22 years. I've followed his path through, and what's most important to me is our ability to take all the things he just talked about and really see that we're embedding that security, now, this privacy, our data protection into our products like we converged everything. We're converging security across everything too, and I think that's really important so that we don't have to expect other people to take care of it, but that the technology does its part and protecting and having authorized use for privacy.

Michelle Dennedy: Yeah. I think that's such an important point. As we talk about more and more digitization and the information, economy, and almost this fluid business decision-making on top of all the hardware and services, the hardware and the services underneath it still have to produce quality results. I couldn't have say it better myself, and I think if you want to reach Paradise with your own SDL or Security or Secure of Software Development Lifecycle program ... Easy for me to say not.

I can't think of anyone better to speak with than Ed Paradise himself and Lisa Bobbitt who bobs and weaves through these issues. These issues are hot topics obviously. I hesitated to say they're hot topics, security and SDL because they're ongoing hot topics. It's like saying food is a hot topic. Tell us a little bit more about what happens when there is a Meltdown in process, when the Spectre of hackers start invading your enterprise.

How do you react with that and how do you exploit those kinds of weaknesses and prevent those kind of weaknesses in a systematic way? I'll start with you, Ed. How do you do this?

Ed Paradise: Yeah. I think Meltdown and Spectre are certainly what's across the newspapers and even primetime news is—

Michelle Dennedy: Can you say what they are a little bit, Ed? I think all of the puns aside.

Ed Paradise: Sure.

Michelle Dennedy: I think it's really fascinating and interesting and a little bit terrifying.

Ed Paradise: Yeah, but I think they're great examples though of what we're dealing with today. Right? Meltdown and Spectre are two vulnerabilities that first came out with the Intel chipset, but also are across other manufacturers, AMD and ARM chipsets. Meltdown is specific to Intel. Spectre, it actually crosses the boundaries, but this is technology that went into microprocessors back in the '90s, so the vulnerability has been there for such a long time.

Michelle Dennedy: Wow.

Ed Paradise: Earlier ... I can't say earlier this year anymore. We're in 2018. Back in 2017, a long time ago, this vulnerability was discovered.

Michelle Dennedy: Way back then.

Ed Paradise: The interesting thing about it, it was four different independent research teams all found the same vulnerability that has been present since the '90s, that was all found late last year. Basically, what a processor is doing to try to improve performance is if you're going to do like an If, Then, Else statement, it's going to follow both paths, and then when it knows the result of the test, it'll discard the path that was false, and they'll follow the path that was true. It turns out that some smart folks and through some very complicated ways, you could learn information about other programs that are running on that microprocessor so that I could steal information from another program that is running close to me. That's the basis of the vulnerability. When you think about cloud environments where you have multiple customers that are running in the same environment, that's where the vulnerability exists.

Michelle Dennedy: Exactly.

Ed Paradise: If I take a look at Cisco's products in the very simplistic case of a router where only Cisco's software is running in the router, then we're not vulnerable to this because there isn't this other software program that is running on the machine that could try to learn what the other programs in the machine are doing, so the vulnerability really exists in a multi-user environment

where one user is going to be able to, with some software that they put on the machine, leak out some information from the Kernel or from other processes on the processor.

Michelle Dennedy: Let me ask you a question here, Ed that is a total curve ball just because it just popped into my brain. We talk a lot particularly in privacy about the collections in the edges, so what we're trendily calling the “Internet of Things,” or IoT networks. We're assuming that they will be multi-tenant or have many people either observed or consuming that information at all times. What I'm hearing about some of these vulnerabilities are that they are exploits of actually how the chipsets were designed so the route to test and the route to share a path and test a path for openness was indeed a feature once upon a time, much like the ventilation shaft at Alcatraz was a feature once upon time, and over time, chipping away literally at sea air saturated cement. People were able to break out or exploit that vulnerability.

What happens in an environment that we have today where we're designing things intentionally to be public? Is this potentially revealing an opportunity to get more secure from the beginning, and really design our services for this issue of multi-tenancy, understanding that when you are living with data communally in a cloud, you're going to have different needs and desires and degrees of exposure? That's a huge mouthful, particularly for a podcast, but that's what just popped in my mind is like this isn't really bad design if you look at those chips. It's how they were designed in the '90s and the application of today is really where this exploit comes in.

Ed Paradise: Yeah. I think you're exactly right. There was a blog that came out last year, and that, all those four independent researchers read this blog and say, "Here's the air shaft." Right? The issue for the microprocessor was this processing that I'm going to go down these multiple paths and throw one away.

Michelle Dennedy: Yeah.

Ed Paradise: The one that I threw away, I didn't really necessarily clean up all of that data that was there, so then folks said, "There's data sitting there. Let's go figure out how to get it", and they put their minds to it, and went and found it. Back in the '90s when the engineers were figuring out, "How am I going to make this processor faster?" They have no idea that this is going to turn into an exploit, but that's what Secure Development Lifecycles are all about, and it's not a static thing. There's feedback in that lifecycle from our white and black box testing, from what customers find so that it's evolving. You've got requirement that we've put in place for our engineers to follow through this process are constantly changing.

The bar is rising continuously because we learn more every day and we put some safeguards in, and then somebody figures out how to beat that safeguard, and we've got to put further protections in, try to beat them to increasing our protections before they figure out the original one.

Michelle Dennedy: Yeah. I want to inject here much like a vulnerability, because I think the thing, and this shows you our wiring, Ed, and this is why I love, love, love working with you is I hear this stuff, and then my weird data brain comes in on this. You said a couple of things about a speculative processing and the design for speed as quality, and then I think the other thing that's really raises the Spectre in me so to speak that I'm going to address to Lisa is this notion of data and visibility. We

hear this all the time from marketing people mostly, saying, "I don't know what data I want. I'm going to keep it all forever."

When you do have that excess data alone hanging out and you do find a vulnerability that has access to data, it may be an unused credential for an employee that's left the business. It may be a pile of contact data from a conference that no one even remembers attending anymore, but when you have the speculative processing and the power of cloud behind some of these speculations, what is the role of data visibility and privacy engineering mixed in with this SDL methodology?

Lisa Bobbitt: RSDL's had as Ed is coining, RSDL is always morphing, and it's morphing into handling the sustainability of those clouds and that environment that we're working with, and how long do we need to keep data, so we have to actually expand our lifecycle to, "How much do you really need to keep?" Like scope that data at the beginning to, "How soon do you throw it away? How long do you retain it, and how do you throw it away? Do you truly delete it, or do you just unplug it kind of stuff from its pointers?" That's what the nice thing about the CSDL piece of this is. We've always had data requirements in the CSDL, but now that we're focusing even more in cloud, in IoT, in the environment which has some things on the customer's prem, some things at Cisco, we have to really start focusing on how that data lifecycle lives through that CSDL and practice good security on it. What's nice about it is the CSDL is built such that we can be embedded into it, versus building something separate for privacy and data protection. It actually just all fits into our development lifecycle, which I call now my “data lifecycle,” so I try and say--

Michelle Dennedy: Which I like. See, I've infected her, Ed. First, I stole her, and then I infected her.

Ed Paradise: Yes.

Michelle Dennedy: Ed, let me ask you this. As part of the product security baselines, which is the bare minimum that that product should meet for quality coming off the line in the Secure Development Lifecycle, what are the 'Ah-ha’s for you when the concept of privacy and engineering were first introduced? I mean, you're always evolving, and then all of a sudden, these crazy, some of us, liberal arts majors come rolling into your data center, and saying, "Hey, Ed. We've got a whole new set of requirements."

What is your reaction when we first started coming in and saying, "Hey, we really have to design in the data as an additional layer of architecture."?

Ed Paradise: Yeah. It's interesting because as I said, we continuously morphing to make sure that we cover and make our products more secure, and data privacy is a whole brand new area, and as we roll this out to the tens of thousands of engineers that we have, we've got to be able to explain it to them so that they know what to do, and that's what CSDL is great about. Right? I mean, I think we have been very fortunate that we understood the need. CSDL is over 10 years old and Cisco now.

The way CSDL works is at the very beginning of the product lifecycle, when an engineer and the marketing folks are figuring out, "What is that product or that service or that offering that we want to put together?" CSDL is right there. They're using it. They're going to do a threat model. They're going to understand what the threats are. They're going to go through the hundreds of

PSBs, or best product security baselines, the best practices that we've had, and they're going to know, "How does that catalog, that they need to do these 116, and that these, some are completely mandatory for every offering that we have, and some are depending upon the used case, depending upon where it's going to be sold and what markets, et cetera, so that whole mechanism is in there, and it's part of the muscle memory of development now, and so we could take these new privacy requirements and inject them into that system to have a very positive outcome, and give the teams the help that they need so that they could be successful.

One of the simple requirements that we have for every product that comes out of Cisco in the privacy's field is know what personal information you are handling. Right? That sounds very simple, but it's different. If you go back in time to our earlier days, we were selling a box.

Michelle Dennedy: Right.

Ed Paradise: That box went out to the door, and it was in our customer's environment, and our customer put their data on it, and we've been, have a lot of involvement with their data. Today, that's completely different, is the world is moved to, "I want to buy your valuable content as maybe as a service offering, and I'm going to pay for that service, and I'll pay more this month, and use more, and less next month and use less," but that box is now maybe sitting out in the Cisco's premise, and/or maybe operating box for our customer, and their data is now in our presence, and we better know what information we are handling and how to handle it, so it's a whole new world, and tomorrow will bring a whole another new world to this as we learn more and better protect our customers.

Michelle Dennedy: Yeah. Hey, Ed, there're tens of thousands engineers. What do you think of that idea that IP addresses are personal data?

Ed Paradise: Yes. Exactly.

Michelle Dennedy: I mean, that's one of those big things that we've just had to really teach awareness to them, and having things like our Ninja program that allows us to go out and teach about these concepts has been really a part of a big piece of the awareness that CSDL brings to our story. Right?

Ed Paradise: Yeah, and it's that foundation that we have that we leverage, and that that's what makes us, it gives us the capability to scale.

Michelle Dennedy: Yeah.

Ed Paradise: The other thing that it helps us scale is the digitization of this, because as any security team would tell you, vulnerability gets discovered in a network.

Michelle Dennedy: Exactly.

Ed Paradise: Right? You don't have a whole bunch of time. You've got to react quickly. You've got to react with tools, so it's the same thing that's going on is when we're developing our products. Right?

The tools have to be there, so I'm going to release that code, so up on the website so all our customers could download the latest version of software. Before I do that, I've got to make sure

I got to rescan that code, that there's no vulnerabilities, and there's a whole host of things that have to happen. That has to just happen. It can't rely on a person doing something. It's got to be embedded in the system. There's got to be milestones and locks in the system that you don't get to the next step until you pass these things, and that's what makes this work and that's what makes it scalable across a company that's as big as Cisco.

Michelle Dennedy: It's Agile, and we're working with DevOps like we do, so you're exactly right. Ed, I'm hearing a lot of passion from both you and Lisa, and so I'm going to wrap up with you like we do all our guests and say, 25 years and, man, you're still excited. You're jumping around and learning and evolving, and what gives you hope for the future? What keeps you motivated and this excited and passionate to lead not only this really important effort, but also, Ed is our site leader for thousands of families depend on your energy and your leadership. Give us, roll us out with 30 seconds of wisdom, man? Bring us to paradise.

Ed Paradise: I think it's really simple. I mean, the passion and the excitement comes from the outcomes that we enable.

Michelle Dennedy: Yeah.

Ed Paradise: I mean, look how our lives have changed, and the change is happening so rapidly. There's the exciting part of it that, "Who could predict what's going to happen next year or the year after that?" That unpredictability with the speed that we are moving just excites me, and what we've been able to accomplish has been tremendous, but what we're going to be able to accomplish next year and the year after that is just so cool, and that's what I look for too and want to be a part of, and we've had a very positive impact on the world both from a technology perspective and from just working with charities and helping people and totally non-technical ways is what I've been proud of and want to do more of.

Michelle Dennedy: That's amazing. Amazing. Thank you so much both Lisa and Ed for your time this morning. The closing thought I have is, I mean, you've got ninjas, you've got digital, you've got hijinx, you've got international crime. What more could you want from your podcast, man?

I think the other thing I will thank you in particular, Ed is you're also such a champion for inclusion, and just as we've recently passed up, January 6, 2018 was the centenary mark for women in the UK and Ireland, but only women who had property, mind you to go out longer for others to receive their right to vote. We still had to wait three more years here in the U.S. for our centenary mark, but I think it shows you there's so much progress here. Inclusion of voices is always high in your list, and I appreciate your thoughtful mentorship and your leadership, and I share your passion with just fun things on the horizon. Thank you so much. Thank you, Lisa too.

Lisa Bobbitt: Thank you.

Michelle Dennedy: You've been listening to Privacy Sigma Riders, brought to you by the Cisco Security and Trust Organization. Special thanks to Kory Westerhold for our original theme music. Our producers are Susan Borton and David Ball. You can find all our episodes on Trust.Cisco.com, or subscribe wherever you listen to podcasts, then please, take a moment to review and rate us on iTunes. To stay ahead of the curve between episodes, consider following us on Facebook, LinkedIn, and Twitter, and you can find me, Michelle Dennedy, on Twitter @mdennedy. Until next time.