Carnegie Mellon University
Software Engineering Institute

SEI Podcasts

Conversations in Software Engineering

Asking the Right Questions to Coordinate Security in the Supply Chain

featuring Carol Woody as Interviewed by Suzanne Miller

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

Suzanne Miller: Welcome to the SEI Podcast Series. My name is Suzanne Miller, and I am a principal researcher in the SEI Software Solutions Division. Today I am joined by my friend and colleague Dr. Carol Woody. Carol is a principal researcher in the SEI CERT Division and a frequent guest on our show to talk about her work.

Today we are here to talk about Carol's work on the Acquisition Security Framework [ASF], which helps programs coordinate the management of engineering and supply-chain risks across system components including hardware, network interfaces, software interfaces, and mission capabilities. Welcome, Carol.

Carol Woody: Thank you.

Suzanne: As I stated, you have been a frequent guest on our podcast but not everyone knows who you are. Could you tell us a little bit about yourself, what brought you to the SEI, and the kind of work you do here? Especially, tell people what is the best part of your job.

Carol: My prior work experience is system and software engineering, and program management. The CERT Division hired me in to help build capabilities that integrate security considerations into the acquisition and development lifecycle. Supply-chain risk has become a major concern. We are seeing that as a growing attack vector, and so that is the focus of our current work. I enjoy the fact that we can really identify key problem areas that need attention and focus a lot of expertise in those areas to help programs.

Suzanne: OK. In a previous podcast, you talked about how increasingly the provenance of code is through the software supply chain via code libraries, open-source third-party components where reuse is rampant. I would say most of this talk about it as being the Wild Wild West out there in terms of understanding what is in the software that builds the software that builds the software that we actually are trying to use. These reuse codes contain defects that are unknown to the new user, which in turn propagates vulnerabilities—See? I have learned from speaking with you—into new systems. How does this current environment impact the cyber risks associated with software-reliant systems, especially systems designed to operate in large complex environments and what we would call systems of systems [SoS] where they are interacting with other systems as well?

Carol: Well, the reality is that we are now fielding software-reliant systems composed of hundreds of components, and all software contains defects. Our research has shown that at least 5 percent of these defects can become vulnerabilities that would allow an attacker to compromise the confidentiality, integrity, and availability [CIA] of data critical to a system's performance. As more of the components come from third-party sources, the success of this fielded system then becomes dependent on the processes and practices of these third-party organizations and how well they identify and fix problems, as well as the capabilities of the system's owner to monitor when things need to change, apply updates, and quickly and effectively address issues as soon as they identify them, which may mean shutting down things and functionality until the third-party vendor has a fix available. It is a whole different risk perspective. The challenge is that many vendors do not provide timely fixes, and many organizations do not apply fixes in a timely manner. This results in a continuing increase in our supply-chain risk. Managing this, identifying it, puts programs at risk with a lot of things that are inherited as opposed to things they can directly control, and managing that environment is quite challenging. A lot of our existing methods and approaches don't effectively focus attention on this problem space.

Suzanne: I was talking with some colleagues, just informally, and we were talking about technical debt, which is obviously related. As we don't apply fixes, we are adding technical debt to our legacy systems that needs to be addressed, etc., etc. We were talking about the fact that you get into this quandary in systems development where you are developing new code, and then you have got this existing code from a maintenance perspective or from something you are reusing, and how do you navigate that? But interestingly, in that discussion, we said nothing about security. I think that is what you are highlighting here is that we have all of these risks that relate to security, but we just don't have it in the front of our mind that other things like supply-chain risk…We think about supply-chain risk in terms of availability a lot of times, but we don't think about it in terms of security. This is one of the things that having a framework that helps us to focus on, *Have you thought about this? Have you thought about that?* is one of the things I am seeing as a big value add to the community that is developing and sustaining software because most of it is in the sustainment right now anyway.

A couple of things that relate to this to try and help us to make more focus on security, we did have, in May of 2021, the White House released an Executive Order 14028 called *Improving the Nation's Cybersecurity,* which focuses on security and integrity of the software supply chain. This is a huge win, just even having an order that even addresses the topic, and it emphasizes the importance of secure software-development environments. That was followed in September of 2022, the White House issuing a follow-up memo for agencies to comply with any misguidance that results from the executive order. Tell us how your work connects to this and helps federal agencies secure their software in response to that executive order.

Carol: Well, we certainly have visibility in terms of the priority that is being put on addressing the supply-chain challenges.

Suzanne: Right.

Carol: But one of the challenges that the programs are dealing with is that the guidance is of necessity very broad because it has to apply to a wide range of environments that consider many, many options. But each specific system and acquisition program has to determine how to apply that guidance to their unique structures, lifecycles, and supply chains. Typically, the responsibility for this is spread throughout the organization. They have got ways of doing business that they automatically follow. Those are their standard practices. Many hands touch the software, many are involved in selecting supply-chain components. In reality, no one has strict responsibility for ensuring that all of these parts and pieces are coordinated. In many cases, the supply-chain risk is being lost in the midst of all of this parceling out and parting of pieces. Every vendor is also using third-party components. There is this dependency on how well the supplier is managing their supply chain as well. Typically, contracts are silent in terms of how this supplier needs to inform you in terms of what they are doing, so that you are at least aware of the risks. All of these are pieces that a program office has not had to deal with in the past.

Suzanne: Right.

Carol: They have been focused primarily on cost and schedule. What we have been looking at with this framework is how to put the right attention to these issues in the right place where people have the right responsibilities. It involves a tremendous amount of coordination among the program level, the engineering level, the development level, support. *Where is your infrastructure? How are those decisions integrating with what you are actually using to build the products*, and *Who is making selections of what code gets included where*? All of these are key players that need to work together, and that coordination has not really been highlighted. Most of these areas function in stovepipes and pass things along through electronic means or, *It is in the library, go get it.* That doesn't really ensure that everybody is treating all of the supply issues consistently. That is where we are trying to put our focus to help programs figure out how to manage this.

Suzanne: One of the things I have noted in acquisition programs, large acquisition programs that I have been associated with, is there is this differentiation between acquisition and procurement. When we get into the procurement side, that tends to be things that are considered kind of off-the-shelf things that are routine that we do a purchase order. We have a relationship with a supplier, and we just call them up and get them to invest.

It is never that simple in the government, close but close to. One of the things I have noted is that we have lots of training and resources that are focused on the acquisition community. But that procurement community is one that I suspect is part of this whole supply chain because when they order a chip, a component for a piece of hardware, they are not thinking about it as actually having firmware in it and having a software component to it. They are not even thinking about the software supply-chain risks associated with that chip. This is broader even than we think about. Go ahead.

Carol: It is but I don't want to expand it too broadly because, otherwise, we will get into something that is overwhelming. Because in reality…

Suzanne: True enough.

Carol: You have to prioritize.

Suzanne: Yes, OK.

Carol: The reality is that procurement needs to know where that piece is going, and frequently they don't have that information. If it is going into a major system and becoming a key component of your development pipeline, then suddenly it takes on a whole different risk than if it is going into a standalone office, and it is going to be used by one person.

Suzanne: Gotcha.

Carol: It is that coordination level that we are not seeing happen. We sre seeing things treated like commodities but, in reality, they are components of other things. How they are linked together and what you are doing with them is what somebody needs to have responsibility for managing.

Suzanne: This, as you said, can be overwhelming even if we don't expand it out as far into the commodity space. You published a technical note in November of '22 called the Acquisition Security Framework [Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk]. This is the document that is sort of the first public version, version 1.0 of the public version of the framework for use for the purposes we just talked about, enabling people to actually act on this guidance and the executive orders and such. Tell us about the framework itself and how it addresses some of the supply-chain issues you and I have just been talking about.

Carol: We focused initially on the key areas that we have seen as part of the growing supply-chain risk. There has been extensive work for many years on supplier risk management in the operational environment. But recent attacks, such as SolarWinds, are leveraging vulnerabilities in earlier lifecycle stages, which are largely unaddressed by a lot of the current supply-chain practices. With a team of experts from acquisition, cybersecurity, and supply chain, we were pooling that knowledge to identify what is really needed in these early lifecycle stages, which would involve program management, it involves engineering, it involves support, and compliance for the effective supplier interfaces and management. Process fits into that as well although some of that is a little fuzzier in terms of how to structure specific supply-chain issues around.

The framework is structured as a series of questions, and we have initially published the information on program management, engineering, support, and process. These areas then can be looked at as questions to probe into current practices to identify gaps and identify ways that may need improvement. Hopefully, you will find in many areas that you are already doing a lot of these practices. Or, we see that they are doing them but they are incomplete, so it just involves some augmentation. It is not like it is something brand new that nobody is doing. It is usually that it is buried in places, some of the coordination is incomplete, there are other areas that need to be brought in, or it may need some overall management to just make sure information is being shared effectively because we have to highlight what is becoming a risk. Not everything is a risk. There are some very good suppliers, and we have been relying very effectively on a lot of third-party software for a long time. This is certainly not trying to shine a spotlight on supplier interfaces as a risk. But it really is trying to help programs grapple with, *What is it I need to do? Where am I missing pieces?* and*, How do I make this coordination happen so that I can effectively apply all the guidance that needs to be in place?*

Suzanne: OK. As you said, that may not be all the topics but process, engineering, management, certainly coordination support is a pretty hefty start at looking at all of the areas that we need to. My read of things is much of what you are talking about is making things that might have been implicit in the way the organization was being managed and coordinated and trying to raise those up to something that is explicitly seen. Once you see it, you can deal with it in a more coherent way, in a more holistic way. That was my impression of the framework.

Carol: Too frequently, there is an assumption that coordination is happening. We are trying to shine a spotlight on key areas where we know coordination is critical and making those more visible.

Suzanne: OK. I know in your work you are very big on getting out into the real world and piloting the work before you really say it is done in any fashion. Where have you piloted this framework with organizations or agencies? Have you noted any places that should not use this framework? That is I think something that would be helpful for our listeners.

Carol: I can't say I have identified areas where it should not be used. But what we would suggest is that you are really looking at, *What is the concern area around supply chain? Where are you in the process of managing your suppliers?* If you have a very small number and you feel like you have got very good relations with them, and you have a good level of coordination among the processes in your organization, and you are comfortable that you have sufficient visibility on your supply chain risk, then this may be more of just a cross-check process that would be useful just for you to be familiar with, to make sure you haven't missed something based on what experts have identified as useful. If you are in a situation where you are ramping up a program, expanding a program, moving into new areas, we have seen it most effective in organizations that are expanding quickly because there are a lot of new people coming in, there is a lot of fluid structure that it is very easy to lose some of the coordination points because they are not in common practice. Then it becomes useful as a tool to really look through and periodically verify that you don't have any gaps that could create future problems.

Suzanne: Right. I appreciate that, and I know at least one program I have worked with that did go through very quick expansion to quite a large size. I have seen evidence that not just in this area but in general, that kind of organization tends to suffer from coordination issues. Because what used to be just a hallway conversation between two people, now I have got 20 people in two divisions that have got to figure out how to coordinate the work that is related to that topic. So, I really appreciate that viewpoint.

Carol: Well, there is another aspect too in that quick expansion in that frequently, as a default, you rely too much on assuming the vendor is doing things. That is something that a program office and engineering needs to be able to verify. Do they have sufficient information that they can know that the risks in the vendor supply chain are being addressed? Because we are all learning about supply chain and the challenges with it and the risks as we go along. This is an area that's mushroomed in the last few years. It is not something that most engineers and program managers are experienced with. Some of the programs we have piloted in, we are also seeing where knowledge of the program office and engineering is heavily skewed to one part of the technology or another. They may be primarily knowledgeable in hardware and now, suddenly, they are implementing massive amounts of software. They don't perceive the risks properly. So that they need to be looking at who are the participants to make sure they have the right knowledge in the problem space to make sure they are covering issues.

The same is true if you have been using software primarily and now, you are going more into firmware. That is a whole different set of risk areas that you need technical knowledge and expertise and experience with that. You can't just assume that it all operates the same way. We have too many of those assumptions in the way we organize as if knowledge is plug-and-play, and it's not. And as you pointed out, frequently the conversations in the acquisition and development side don't even think about security risk because we don't have that level of expertise built into those processes yet. It may mean you need to draw on other areas of expertise to come in and put the right eyes on the problem to see the risks.

Suzanne: I think this executive order is actually a step in that direction. Those kinds of things tend to bring a topic to the attention of the senior management who are probably ones that are not as schooled in these topics and make them aware that they have got to deal with this explicitly if they want to be able to show compliance and all those kinds of things that they have to do.

Carol: But that expertise we have seen is not easy to come by. It may mean you have to build the expertise. We are seeing gaps in education and training that engineers and program managers may need to look at, *Do we have the right skill sets, and then how can we grow those skill sets?* No one comes out of the educational system having had any background in cybersecurity. It is just not part of a standard engineering curriculum. We have to recognize that and bring that kind of expertise somehow into the problem space.

Suzanne: I wonder if this is one of those things where 10 years from now, we will look back and say, *Wow, how did we even survive before we had this kind of expertise being taught at the undergraduate level as well as graduate levels?* Similar to Agile. Now everybody comes out of school having some understanding of how Agile works, but even 10 years ago that wasn't the case. Some of those things we may be able to address through education. But in the meantime, as you say, we have got to build that *in situ* with our on-the-job training and other things. Yes.

Carol: There is a problem too in relying on the educational environment because there is a coordination challenge there as well. You have got knowledge that is being built in your business-management side that is funneling into your program managers. Then you have got knowledge in your technical area that is funneling into your engineering. Some of these problems are cross-discipline, and they don't get exposure to that in the educational environment. It only comes to play when you are putting the pieces together, integrating everything, and suddenly trying to deal with the challenges of operationalizing something that has inconsistencies and has a vendor-support problem.

Suzanne: The framework is published. We have talked a lot about the problem space. The framework being published is, as we know, the start of transition of this kind of information out into use and into practice. The SEI is a transition organization as well as research. What are the kinds of things that people should be looking for in terms of resources to use the framework in their own organization? And how do they get started with it?

Carol: Well, in reality, we are at the beginning of a journey. The tech note is really the first major piece that is available publicly. I would recommend reading it through and getting familiar with the questions that are being asked even if it is not something you are prepared to take into your organization and apply yet. Because at least thinking about those questions gives you a starting point.

What we are looking at doing is assembling very specialized, focused subsets of the framework that would deal with problems like the software bill of materials [SBOM], which is another executive-order requirement that has come out that relates to the supply chain but isn't directly tied to it in terms of risk. But if you have a software bill of materials, how can that help you? Or, if you are in the midst of considering committing time and effort to putting a software bill of materials in place, what are the issues you should think about to make sure that it will be useful to you in terms of dealing with supply-chain risk? We are looking at what are the right questions to ask. How do we put this together in a way that it creates something that is more directly usable for a specific problem space.

Suzanne: OK. What about things like training on usage and helping people to understand some of the concepts that are underneath this? Are we participating in that at the SEI, or is that something that we are hoping that the security community in general is going to take up?

Carol: I would say that we will be certainly driving out pieces of that. I can’t give you a timetable for when we are going to be doing that. It is based on a few of us that have resources to roll that out. But it is something that we are looking at very definitely, workshops if nothing else just people involved and accurate.

Suzanne: Excellent. What is next for you? Are you going to continue to work on the transition of the framework, or do you have other research that has you excited that you are going to be transitioning to?

Carol: Well, we are definitely looking at finishing out pieces of the framework, and hopefully, that will be published shortly. We have draft items of those that we are finalizing right now. As I said, we are exploring specific examples. Where I am focusing my attention though is a related area, and that is concerning how do we measure security. That needs to be a piece of the supply-chain consideration as well. Just counting vulnerabilities doesn’t really give us a sense of where we are or what we are doing. Somewhere, we have to look at how do we structure what is it we want to accomplish with security. The reality is the only super secure system is one that nobody is using and nobody is doing anything with, you preserve it perfectly. Otherwise, there will be issues. It is going to be a balancing act; what is good enough? Many of us have been doing that qualitatively. Where can we go quantitatively in terms of establishing more realistic structures and things that we may be able to automate and monitor through automation? That is where we want to go but we have got a long path ahead of us there.

Suzanne: Yes. DevSecOps probably contributes to that, makes some of that easier. Boy that is a much, much bigger problem than just instrumenting a DevSecOps pipeline. You have always been ambitious. You continue being ambitious in your research goal.

Carol: Well, it is probably the problem.

Suzanne: Yes, it is already a problem.

Carol: It is research.

Suzanne: Yes, yes. It is a worthy problem, and I applaud it. I am ready to do a podcast with you on where you are going with that in the next six months or a year. That is something to look forward to. Oh my gosh. Carol, I want to thank you so much for joining us today. I am very excited that this framework is available. I know you and I both have customers that can make good use of this, and we need to get them familiar with it. I hope that our audience also understands the importance of getting this kind of information into their organizations so that they can deal realistically with some of these seemingly overwhelming supply-chain risks. I agree that we can't boil the ocean with this but having a framework that allows us to start asking the right questions, I think, is really a good start, especially for people that really don't have a huge background in this area. So I want to thank you so much.

I do want to tell our viewers that we will include links in the transcript to resources we talked about, the executive orders, etc. Also, I want to mention that in addition to the technical note, there is a blog post available so you can find that on our website as well. A reminder to our audience that our podcasts are available everywhere—SoundCloud, Stitcher, Apple, Google, and of course my favorite, the SEI's YouTube channel. If you like what you see and hear today, feel free to give us a thumbs up, and thanks again for joining 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 don't hesitate to email us at info@sei.cmu.edu.