The CERT Software Assurance Framework

featuring Carol Woody and Chris Alberts as Interviewed by Will Hayes

----

Will Hayes: Welcome to the SEI Podcast Series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally-funded research and development center operated at Carnegie Mellon University and funded through the United States Department of Defense.

I am joined today by two of my colleagues, Dr. Carol Woody and Chris Alberts, who have done some recent work on a Software Assurance Framework. And there's some blog posts and a technical note out there for you all to reference. But we are here to talk about that work. Before we get into that discussion, could I ask you each to introduce yourselves and talk about a little bit of your history? Carol, if you could start.

Carol Woody: I am the technical manager for cybersecurity engineering, and my work is focused on trying to draw from operational security and bring it into the development lifecycle. We are especially interested in strengthening the capabilities of addressing cybersecurity early in the lifecycle when it can be done at lower cost and certainly without all the pain and angst that we are dealing with in terms of operational response to attacks. We are aiming at, *How do we minimize the attack surface and a lot of the security challenges in the operational side through effectively addressing engineering and development, applying good cybersecurity practices?*

Will: Great, thanks. Chris?

Chris Alberts: I am a principal engineer here at the Software Engineering Institute in the CERT Division. I have been at the SEI since 1995. I started in the software risk management area, moved over to CERT a few years later, and started in the operational security part of research where I led the development of the OCTAVE risk analysis for operational systems.

Then, about five or six years ago, I joined Carol and started looking earlier in the lifecycle and really taking that risk management perspective and starting to look at, *How do you engineer practice controls into software-reliant systems, starting really early in the requirements through* *the architecture and design and through the code*? The current work is really looking at, *How do we integrate good cybersecurity practices in with good software and systems engineering practices?*

Will: You have had some good experience with customers. One of the great things we do at the SEI, I think, is engage people who have real needs, and we learn from the work that they are doing using the material we publish. I think the blog post does a very nice job of illustrating pilots you have had. Could I ask you to kind of take turns and talk through the pilots a little bit? And maybe start with Dr. Woody.

Carol: Well, one of the first areas we were looking at was supporting the DoD in their efforts to initiate work in software assurance. So we were asked to identify what practices they were doing that effectively addressed the cyber issues and where there were possible gaps. In order for us to address the gaps, we had to basically structure a baseline to compare them against. We assembled that through a lot of the experiences that we had had in the operational side, tied it back to expertise that we have here in acquisition and engineering to essentially identify what are critical practices that really belong to engineering and development throughout the rest of the lifecycle, and link that up to DoD's acquisitions to give a strong relationship there for a baseline. Then we could identify the engineering practices that were supporting that baseline and potential gaps for them to address.

Will: So it is not just identifying practices but making sure that the timing for the best execution of those practices and the people responsible for them, that you are identifying those linkages. That makes the practices more effective?

Carol: Yes, it puts them where they need to be in terms of who can be the most effective in addressing them.

Will: Great. If I could turn to Chris, you applied Goal-Question-Metric in one of the pilots that I read about in your blog post. I think that would be particularly interesting to our audience. If you would elaborate that a little bit?

Chris: Yes, it is the most recent pilot that we have been working on where we started with the practices and the framework and focusing on the engineering practices. Kind of digressing a second, we have the practices now arranged in process management, project management, engineering, and support.

Will: Familiar categories.

Chris: Yes. That is kind of the basic structure that we followed. So we focus on the engineering practices for this particular pilot activity. What we did is we used the practices in each of these areas as kind of the overarching goals and then constructed a set of detailed questions to elicit a range of metrics. We came up with a large candidate list, and then we worked with the organization to pare down that list to a starter set of metrics that they are now starting to implement.

Will: And that starter set is available in the context of the blog post, and you can see the linkage from goals to questions to sample metrics.

Chris: Right.

Will: I think that is a particularly powerful way of communicating experience that people have had. It goes beyond just the concept and it talks about instances of it.

Could you talk about your other pilots a little bit and maybe pass it back to Dr. Woody?

Carol: The key areas relative to addressing cybersecurity have not been well recognized by high-maturity organizations. One of the areas that we have been looking at is, *How do we articulate what needs to be added to all of these excellent engineering practices to bring them up to the level we need for cybersecurity?*

One of these high maturity organizations came to us to help them identify what practices are missing. So we were assembling for them not only what practices they needed to do, but where did these need to be integrated into their current policies and procedures so that they could make sure that they were not losing the quality efforts that they already have in place.

I think one of the real telling points that came out of our review of that is that there really needs to be someone who owns the responsibility for software assurance and cybersecurity across the lifecycle. Right now we have people that own process improvement. We have people that own configuration management and certain responsibility areas that are cross-cutting. We really need someone that owns the cybersecurity responsibility. Traditionally it has been left to the security operational side.

Will: After the product is out.

Carol: That is way too late, and so actually building it in and integrating it requires transferring some of that responsibility earlier.

Will: So you have a focal point. I think there was an observation in your blog post about requirements and how we might think about requirements development and requirements management in light of these needs; could you elaborate that?

Chris: Yes. I think before I get to that, the broader point of view is we do not think of security as an add-on. So we want to integrate it into the process, and requirements is a very good example of how we did that. We looked at the requirements development process, we noticed that some of the good practices that we recommend for generating security requirements were not covered in the current processes. So we recommended that they create an add-on process or integrate that perspective into their current processes or create a separate one. It did not matter how they did that, but they needed to address that.

So from the development point of view, then they could develop a good set of security requirements. But from the management point of view, we felt that with the current processes they had in place, they could handle the security requirements and manage them just like they manage every other type of requirement.

We identified areas where they needed to integrate security in and areas where what they had was sufficient. But the one thing that philosophically we did not want to do is say, *Here is your cybersecurity process. It is stand-alone from everything else.* It is integrated in with all the things that they need to do.

Will: So, along with the responsibilities being focused on a person who is charged with these things, the fact that processes are able to accommodate requirements relating to security in a high-maturity organization was particularly encouraging. The different perspective that people bring when they document requirements or elicit requirements relating to security—could you contrast that with the way people think about requirements for a product's functionality? And how different is that perspective? The person who, Carol, you talked about being the focal point versus someone who is a product manager, perhaps.

Carol: Some of it relates to how we do good engineering nowadays. Traditionally, engineers have been trained at both the systems and the software level to decompose pieces down to components and build the components effectively to meet the requirements.

What we are seeing with cybersecurity, though, is that it is really how the components are integrated and how they work together with the infrastructure, as well as the user operational interactions that either protect the structure and environment from an attack or provide holes and conduits for attackers to get to data and functionality that we do not want them to get to. So we have a mindset that is built in to the existing practices that they are very componentized and subdivided. And it is this cross-cutting look that is missing relative to security.

Will: It is not the unforeseen behavior of an individual component; it is the combination of them and the unforeseen things that could happen there.

This is very much in keeping, Chris, with the work you have done of taking risk and going earlier in the lifecycle with risk and going to places where decisions are made or failed to be made early on. This really is a continuation of the focus you have had. Could you elaborate a bit about risk here?

Chris: Yes, sure. The focal point of most of the techniques that we are doing right now are risk-based. What we are doing is essentially looking at how the system likely will be used. Let us say that we are building a system or acquiring a system that is software-based. We want to know how that might be used in operations. What mission threads it might support and how it would support them, and how the data flows through the various system. Because we are really talking about a system-of-systems environment.

Once we understand how data is supporting the mission thread, now what we try to do is we try to figure out how can we break it? It is that attacker perspective that we try to bring into the engineering process and look at if we affect the confidentiality, integrity, or availability of various data flows, what would that do ultimately to the mission thread and to the stakeholders who have an interest in that mission thread? That is kind of how we look at risk.

Once we do that, we identify what are the design implications? What can we incorporate into the design that might be able to counteract that? That can influence the requirements, the architecture, the detail design, and so forth. That is what we are focusing on, that's how we are bringing the risk perspective earlier in the lifecycle.

Will: Great. Carol, I know your contributions to helping people think clearly on these topics and education in general, I think, has been something your work has focused a lot in terms of curricula. Now this new framework is another collection of some pretty powerful stuff. Would you talk a little bit about the audience for the tech note that you have published?

Carol: We really see the audience as being a combination of the organizational level, as well as individual projects or acquisitions. Because the practices really require an integration across what a specific system development activity would have as well as the ways in which the policies and practices of an organization influence that, linked to the way the infrastructure is built and supported.

Because the attacker is not exclusively just focusing on the content of one subset of this process, they are looking at how all these pieces are glued together, which is ultimately what is fielded in the operational environment. So we are trying to take the thinking of, *This is how it is going to actually run and the kinds of exposures it is going to have to deal with* and driving that back into, *You have to build it to accommodate those challenges.*

Will: This is really quite a variety of people who you are trying to reach with the work you’re doing.

Carol: I refer to it as a team sport because you are looking at decisions that engineers are making. You are looking at decisions that organizations are making based on trading-off cost and schedule. You are looking at the competencies that they provide within a development activity. You are also looking at the tools and techniques that they provide and give people time to use, and make sure that they know how to apply them effectively. So there is a wide range of these practices that really have to all integrate across the lifecycle for effective results.

Will: And the work you have done with the pilots that we have spoken only briefly of so far, really, you can see the three instances being described in a fairly diverse group. Now, I saw in the blog post you went from Version 0.1 to 0.2; where are you with the versioning of this product now?

Chris: Well, we are still with Version 0.2. That is the current prototype, and I consider it still to be a working prototype. The idea is that we have done some pilots, we have got internal people assisting us and building the framework. What we would like to do over time is to get more community involvement, grow the product, make it into a real product type, ready for prime time kind of product, and then transition it. That is our long-term focus, and we are just starting on the path towards that.

Will: So the tech note you have published will give people an early look, and it may form a basis for them pursuing future communications with you all—maybe offering input to you, maybe engaging your services to look at how this plays out in their team.

Carol: I think in the near-term we will be publishing more information about the metrics we’ve identified and the potential output documents that those could be reflected in, specifically in the acquisition process to give people an opportunity to try and see how they can manage acquisitions better using some of this information.

Will: So we have covered a variety of good topics here; what have I left out? What more do you want to get to the audience?

Carol: I think one of the key points that I keep running into is that people say they cannot do anything because they are later in the lifecycle. My response is, *Start where you are*. We have basically assembled practices that run the gamut of the lifecycle, and there is no reason to not at least do the ones that you still have time to before you are fielding a system.

That may mean that you carry over risks from earlier things you did not do, but certainly with approaches like Agile and DevOps that are coming into play, you have got these opportunities, then, to address those gaps in the next cycle. So, there is no reason to not get started.

Will: Good advice, I think. Very good advice. Last words from you?

Chris: I guess what I would like to emphasize, again, is the nature of engineering cybersecurity, and as Carol said, it is a team sport, and it requires people with security expertise, people with software systems and engineering expertise working together, and doing it in a way that fits in with the way they are already doing business. If as we have seen time and again when people try to make security a separate activity, it just will not get done.

Will: Good advice. Carol and Chris, thank you so much for joining us today. This has been a great conversation.

Carol: Thanks.

Chris: Glad to be here.

Will: As always, this podcast will be available on the SEI's website, as well as Carnegie Mellon University's iTunes U site and the SEI's YouTube Channel. If you would like to read more about the Software Assurance Framework. You can go to the SEI's homepage at www.sei.cmu.edu and type in the acronym SAF in the search box and it will take you directly to the technical note. Thank you very much for joining us today.