Cyber Security Engineering for Software and Systems Assurance

featuring Carol Woody as Interviewed by Nancy Mead

Nancy Mead: 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 and operated by Carnegie Mellon University. A transcript of today's podcast is posted on the SEI website at sei.cmu.edu/podcasts.

My name is Nancy Mead. I am an SEI fellow and principal researcher in the CERT Division of the Software Engineering Institute. I am here to introduce you to Carol Woody, who is the technical manager of our cybersecurity engineering team also in the CERT Division. She is also a principal researcher just like me.

Nancy: We are here to talk to you about a book that we co-authored, which has just been published by Pearson Publishing. The book is *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*. Let us talk just a bit about how we got to the point where we thought we could actually write a book on this subject.

Way back when I started my career at IBM Federal Systems, where I was involved in software development and software management of large systems, I became a senior technical staff member at IBM. [I] later joined the SEI where I was director of education, and then migrated into CERT because I realized that all of the work we had done in software engineering had not been replicated on the security side. There was no real attention to what happens in the software development lifecycle when you are considering security.

My research work has primarily been in security requirements engineering. I have also led a software assurance curriculum design effort. Again, way back when I got a Ph.D. in mathematics from Brooklyn Polytechnic Institute. So, Carol, how about you?

Carol: My background is in system and software engineering. I have worked in a variety of industries, banking [and] government. I worked for the administration at Yale University, which is a pretty good-sized structure, and I handled all their financials. So, financial management has been my specialty.

My background includes an MBA in finance, undergraduate was mathematics. Then I did my Ph.D. in information systems, actually focusing on risk management and a lot of the areas related to the security problem space. But, I did not really get involved in the security angles until I was hired here at CERT to augment the efforts to drive what we had learned from the operational security side into *How do we build these things so they can be secured?* because right now that is a real tough challenge.

Nancy: One of the big challenges that we face is explaining to our constituency why this is so important. That gets us to the question of why we thought this was a good time to actually write a book on the subject.

Carol: Exactly. I am continually told that we just have to get the systems built. *We need all that functionality. It has to be cheap, and it has to be fast. It has got to replace people, and it has got to get things done quickly. We do not have time for the security stuff because that takes extra effort and costs extra. Besides, we do not have the people that understand how to do that.*

Hopefully our book will begin to support some of the issues of educating the world as to why it is important as well as how they can go about beginning to address it. That is why we were focusing on the practical aspects. I know that there was a variety of people we considered the book for. Maybe we should describe who the audience would best be to read this one.

Nancy: That is an excellent point. One of the audiences that we seldom reach with our writing is the acquisition management audience. They are so concerned with not only developing products but acquiring them, whether it be by contracts or by purchase of commercial software, for example, that we felt it was really time to enhance their education so they would be thinking about cybersecurity and not solely about functionality. That is one audience segment.

Another audience segment is actually the development managers and the technical staff that have the responsibility for building cybersecurity into their systems.

Carol: Well, they are the decision-makers, and if they do not provide the money and the support to make it happen and hire the right people to do it, it is going to be a challenge.

Nancy: It is interesting in that when I first started working in CERT, and I told people I was working on cybersecurity, nobody knew what I was talking about. Now, when it is in the newspapers all the time, everybody knows what it is about. They do not understand necessarily the connection with why it is so important when you are both developing and acquiring systems.

In our blog post, we talked about seven principles that we developed in support of cybersecurity engineering, but there is a whole lot more to the book than that. The seven principles were kind of an organizing framework. What do you think about the other topic areas that we have in the book?

Carol: Let me give a little bit of exposure to the principles themselves. Those grew out of a discussion I had actually with an international audience, trying to explain to them why we were focusing on cybersecurity. All of the written material that they had read focused on all of these security activities, hundreds of them that they needed to do.

The discussion really centered around, *Well, why do we need these things*? So the principles grew out of that because just saying, W*ell, you need to be secure* was not enough. So how does that link with what we need to do? You have got risk issues. You have got trust. You are leveraging a lot of technology that in some cases you do not even understand. So how are you dealing with those challenges?

Your point about the rest of the book, I think, is critical because we have made risk management the driving focus. In essence that is because nobody goes out and just buys security for the sake of security. There has got to be a reason that they need that type of control or structure around the data and what happens with their technology.

But just slapping on a pile of controls does not necessarily get us there. *What are you doing with the technology? Where is your data going to live? How broadly are you distributing information? What kind of people are going to be working with it?*

All of these become part of the decision-making. By the way, *Where are you getting this technology? Are you buying it off the shelf so that you are just taking what somebody gives you and hoping it works? Is it something you are building? And then more likely we have got these Rube Goldberg constructions that are tying bits and pieces together with what is already there.*

So you have got the legacy interfacing with new products that you are gluing together and then streamlining it out in some sort of distribution mechanism that may be somebody's smartphone that you do not even control. Or it may be posted on the web and you do not necessarily control all of the interfaces and access there as well.

Nancy: You brought up a couple of really important points. One is that we want to try to overcome the checklist mentality where somebody gives you a list of controls and you pick some that you think, oh, might be okay for your system, and then again, might not. Also, the supply chain issue, *Where does the software come from? How many people have touched it in how many different countries? What mechanisms were in place to make sure that it was done with security in mind?* Often people do not really have a clue as to what that supply chain looked like. And that is an area where we really want to have some impact.

Carol: What we are also looking at how people are building software—it is a major planned process. But where in this process do they plan for the security they expect to be there at the end? If it is not integrated across the life cycle, there is no reason to assume it is there once you field the system.

Yet, in reality, our infrastructure and all of our critical support systems as well as all of our day-to-day operations—whether you are a small business or a large corporation or the government—is living and dying based on the technology.

You get an outage because somebody else happened to have created a denial of service and suddenly you can't operate. You have to think about those things when you are building the pieces to field in the first place. Otherwise you are going to get it by accident, and that does not usually get you what you need.

Nancy: The other thing that happens, of course, is that if you have not considered security initially, there is a possibility that you will not be able to incorporate it later on because you've made decisions that preclude you doing a good job with security. We have heard of cases where whole systems were scrapped because they could not be made secure. So that is something we want to help people to try to avoid.

Carol: Or your sustainment costs are huge because you are forever in this patching cycle. We all really get tired of the patching cycle, and that seems to be a way of life these days.

Nancy: Along with the side effects because maybe the patch causes some other problems to emerge…

Carol: Or something else.

Nancy: And people are afraid to apply the patches and leave themselves vulnerable as a consequence. One area that I think was good to focus on was how to help our staff improve their capabilities by testing their competencies in cybersecurity. We also looked at how organizations can assess their competency to build cybersecurity in. I think those were nice additions to the book as well.

Carol: What we are hoping is that it will provide a sequence of how to tackle these things, more of a starting roadmap. Because otherwise you see these organizations just freeze because there is so much to do, they do not know what to do, and they end up doing nothing because they do not feel like there is any way the small amount that you can devote to it will make any sense to bother. If there are small incremental steps that you can start, each improvement is valuable. It makes each iteration a little bit stronger and a lot more manageable as we move down the road.

We have got to start tackling the volume of security problems. Maybe it is only baby steps to begin with, but if you do not take those, you are never going to get there.

Nancy: That is one of the things that we did as a summary of our book, is to talk about how people could start to implement some of these practices and perhaps what order they could do it in, so that it could be most effective and not too painful for them to get into.

Carol: It is going to be painful no matter what. All the pushback I get every time I am working with organizations is, *Oh, there is so much to do; can I just do a small piece*? *Yes, you can, as a starting point, but then you have to grow and build. It is a journey. It is not a one-stop shop.*

Nancy: I think the other aspect of the book that I enjoyed from a writing perspective was talking about some of our more recent research and giving people ideas of what they might consider in the future once they have gotten themselves to a certain comfort level.

Carol: Also what this book provided us is a way of combining information that had been scattered in many different areas. Because you and I both have been writing in this area, producing papers and blogs and a lot of content presentations for conferences, etc. for many, many years.

This allowed us time to sift through that, coalesce it, and put it together and certainly supports the curriculum effort. Because one of the comments we kept getting when we were trying to push out the software assurance curriculum was, *Well, there is no textbook*. This now provides a textbook, so at least that gives us a base to build from there.

Nancy: That is a good point to link back to the audience perspective so we are not just aiming as practitioners but also educators who might be looking for a textbook to use in the classroom when they are doing software assurance or cybersecurity courses. So I think that is a great addition.

You mentioned that we have given a lot of talks at conferences. Well, many times at conferences we are preaching to the choir.

Carol: True.

Nancy: We are talking to other researchers and people who are already working in the field. They do not necessarily need the leg up that we are trying to provide them with the book. I think it hopefully will be a great addition to people not just on their bookshelves but also in practice.

Is there anything important that we have left out?

Carol: Not that comes to mind immediately. Certainly we hope that a lot of people will benefit from at least reading parts of the book, even if not all. It may not be one of those you want to pick up and read front-to-back. There is a lot in it. But certainly it covers a lot of territory. Our reviewers were especially positive in terms of its aim and audience and content.

Nancy: We had a nice group of reviewers, both from the United States and internationally, and from industry as well as DoD, so that was terrific. One thing that I think is noteworthy for our viewers and purchasers of the book is that by purchasing and registering the book with Pearson, they get access to our executive overview video course, which is a really huge bonus for them that is available on our online training program. I think people would really enjoy taking a look at those videos, some of which include you.

Carol: Yes, I know. They might get tired of listening to me, though.

Nancy: Oh, no, never.

Carol: Well, thank you.

Nancy: Thanks so much for joining us today. Our book, *Cyber Security Engineering: A Practical Approach for Systems and Software Assurance*, which we have already mentioned, has been published by Pearson as of November 2016. You can find it on the Inform IT website, and you can also find it on Amazon if you are so inclined.

It is part of the SEI Series in Software Engineering. We are going to be including links to the book on Inform IT, as well as Amazon, along with other resources that we have referenced during this podcast.

This podcast is available on the SEI website at sei.cmu.edu/podcasts and on Carnegie Mellon University’s iTunes U site. As always, if you have any questions, please feel free to email us at info@sei.cmu.edu. Thank you.