At Risk Emerging Technology Domains

featuring Dan Klinedinst as Interviewed by Eileen Wrubel

Eileen Wrubel: 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 sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University. A transcript of today's podcast is available on the SEI website at sei.cmu.edu/podcasts.

My name is Eileen Wrubel, and I'm the tech lead for the SEI's Agile in Government program. Today, I'm joined by Dan Klinedinst, who is a vulnerability analyst in the SEI's CERT Division. Today, we are here to talk about Dan's latest work, which is the 2017 Emerging Technology Domains Risk Survey, which summarizes our understanding of future technologies. Dan thanks for being here today.

Dan Klinedinst: Thank you.

Eileen: So before we get started, could you tell me a little bit about yourself, your interests, your background and what led you to the work you're doing.

Dan: Sure. So I got involved in cybersecurity about 15 years ago. At first I was doing sort of general security. Then I got into doing what's called penetration testing, which is taking an adversarial look at a company's networks trying to find the vulnerabilities in them before bad guys do. I did a lot of that work here at CERT for a few years. Then, eventually, I moved into doing vulnerability analysis, which is stepping back a level and trying to find the vulnerabilities that the penetration testers would look for in live networks. Instead of going out and trying to break into things out in the field, now I sit in my office and try to break into things.

Eileen: Break into things from the inside before they're found.

Dan: Yes.

Eileen: OK. So let's talk a little bit about emerging technologies. You published this report on at-risk emerging technologies. My understanding is this is an annual report that you've developed for the last few years. Can you tell me, how did that come about? How do you do the research, and how is that information put to use?

Dan: Sure. The genesis of this report was a couple of years ago, as you said. The Department of Homeland Security, US-CERT came and asked us to do some research in this area.

Now US-CERT is the government computer emergency response team, which is responsible for coordinating incident response and vulnerability coordination across the U.S. while CERT, specifically the CERT Coordination Center here at Carnegie Mellon University, does research to help support their mission.

They came to us and said, *OK we realize that no longer are security and network incidents just based around computers and traditional IT networks. Now we've got these mobile devices that are going everywhere. Even worse, now we have computers going into virtually everything around us, all sorts of things embedded in cameras and toys and all sorts of things.*

Eileen: My refrigerator.

Dan: Your refrigerator, sure. They came to us a couple years ago and said, *Could you try to take a forward-looking approach and tell us what the important technologies are going to be over the next few years that we should be worried about now so we can get ahead of these threats?*

That was the initial request, and they didn't have a firm way of how we should do that or anything. So the methodology that we sort of developed for report originally was we took something that's called the Gartner Hype Cycle, which basically covers, I think, something like 1,500 technologies on average each year. They talk about how soon they're going to reach the point when early adopters are using them, market saturation. Is there going to be a point at which they have passed their peak of usefulness or where they just become sort of a commodity in the marketplace?

We used that as a baseline and tried to identify the ones that were fairly near-term and had interesting or novel security risks attached to them. We have redone that every year. We go back and look at the newest year's Gartner report and pick out the technologies. We start with a few dozen of them and then try to narrow them down by what seems like it is going to be important, especially in the likely 2-to-5 year range, maybe a little bit out of that if it's going to be, you know, a really big deal. We are focused on things that are actionable now not something that's going to be popular 15 years from now.

Eileen: You do this every year so each year builds on all the years prior, but it doesn't erase it.

Dan: It doesn't supersede it, correct. This is the third year that we've done one of these, and all of the things in the first year are still important. You know sometimes things will fade away a little bit or become a little bit less relevant, but for the most part, everything that we have warned about in the past is still an issue today. But obviously new technologies are coming in being adopted all the time. So we try to refresh that each year.

Eileen: OK. I understand that you identified eight emerging domains this year. We don't need to talk about all of them, but I'm wondering did any of this surprise you. If I am a government agency or defense program what really should be on my radar?

Dan: What we said in the report and what I personally think is that the two things that surprised me—in the sense that they're coming much faster than I expected—are robotics and machine learning or artificial intelligence.

Just three years ago people were saying *Oh, some day we are going to have self-driving cars.* Now we have self-driving cars on the streets right here in Pittsburgh.

These things are moving much quicker than I think a lot of people expected, even Gartner, which isn't to say that the other technologies aren't interesting or novel or are moving quickly.

I'm personally surprised that I'm living in an era when there are robots and artificial intelligence around me.

Eileen: We have multiple self-driving car companies in Pittsburgh anymore. It's not just one platform.

Dan: Self-driving cars are a perfect example of the fact that they need to use both robotics and machine learning to operate. There is this convergence of technologies.

Another of the fields or another of the domains that we talked about in the report are intelligent transportation systems, which is stepping even past the self-driving cars. You've got cars on the road that are also trying to coordinate with trains and pedestrians and bicyclists all using digital information being fed into some sort of machine learning background. We included that partly because transportation is very important. There's actual risks to people because of cars and obviously pedestrians. The risk is important, but also it is an interesting place where robotics and machine learning are coming together.

Eileen: That is really cool. Do you have visions of that tying in at all with the smart traffic research work on campus?

Dan: Yes, so campus is doing some work on some smart traffic signals. They've got a pilot set up here in Pittsburgh, which attempts to manage traffic better by changing traffic lights based on rates of traffic flow and number of pedestrians waiting to cross, when is a bus coming, things like that. That information is going to be used by itself to manage traffic. Initially it was funded by the Department of Transportation to try to take that information and share it with any vehicles that are around it on the road. It is called vehicle-to-vehicle and vehicle-to-infrastructure technologies. They are already testing this out to try to…As your car comes forward, your car is going to know that the light is going to turn red in 10 seconds, and it may take some action eventually based on that.

Eileen: That is going to change the way we live.

Dan: Yes, it absolutely is. That is the great thing about being here at Carnegie Mellon is that we are right here in the hub of where they are doing all this different research.

Eileen: So speaking more about research, is the work that you're doing on this influencing the research strategies at CERT? If so, can you talk to me a little bit about what projects or what areas you might be working with?

Dan: Sure. Yes, it absolutely is. One of the main reasons that US-CERT asked us to do this research originally was that we were to tell them what kind of research we should be working on. *What is high priority?* Of course, they decided what they thought was priority, but they wanted a research-based approach to decide what should we be looking at as we move forward.

Out of the first report, one of the things that was in the report was connected cars. This is really the cars that you have now that already have a cell phone in them. They can do navigation and maps. They have some Internet connectivity. That directly led us to start doing research in cars and vehicles. We are moving towards autonomous vehicles. Over the past year or two years, we've done a lot of research in to cybersecurity vulnerability in different types of vehicles and systems that go in to vehicles. That is one example of where this report directly caused our research to go in a specific direction.

Eileen: That has got to be really fulfilling, to see the needle move as a direct result of your work in this area.

Dan: It is really nice to be involved in all steps. We identify things that are upcoming. Then, as they get more important, we start doing some research in that. Now, we start actually putting out research or advisories or recommendations that are relevant to things that are really happening in the real world now.

Eileen: That's great.

Dan, thanks so much for coming to sit with me and talk about this today. Dan also recently authored a blog post on this work. That can be found at insights.sei.cmu.edu. Click on the author's tab and find Dan's last name, Klinedinst. It starts with a K.

Please know that we'll provide links to these resources in our transcript.

This podcast is available on the SEI website at sei.cmu.edu/podcasts. It is also available on the Carnegie Mellon University's iTunes U site and the SEI's YouTube Channel.

As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.