The Future of Cyber: Security and Privacy

featuring Dr. Lorrie Cranor as Interviewed by Bobbie Stempfley

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.

Bobbie Stempfley: Good afternoon. My name is Bobbie Stempfley and I'm the director of the CERT Division at the Software Engineering Institute. My guest today is Dr. Lorrie Cranor. She's the director of CMU's CyLab Security and Privacy Institute. She also directs the CyLab Usable Privacy and Security Lab [CUPS] and codirects the MSIT Privacy Engineering Master's Program. In 2016, she served as the chief technology officer of the Federal Trade Commission in Washington, D.C., and she is the cofounder of Wombat Security Technologies, Inc., a security-awareness training company.

You are busy. Thank you for being here today, Dr. Cranor.

Lorrie Cranor: Yes, thank you. You can call me Lorrie.

Bobbie: This podcast is really focused on exploring the future of cyber and privacy and trying to take lessons from the past, seeing what can be applied and where we have to take breaks from the past. I am really excited about having you here today, because this triangle of cybersecurity, privacy, and usability seems elusive, and it seems to be the pivot point for your career. Do you want to tell us a little bit about what you have been working on?

Lorrie: Sure, yes. I have been working with lots of students and faculty at Carnegie Mellon to try to solve some of the human problems related to security and privacy. On the security side, we have done a lot of work with authentication and passwords. Basically, trying to make the best of the bad situation we are in with passwords, so that we can have passwords that are both secure and more usable than they typically are. On the privacy side, we have been looking at privacy policies and privacy choice options and how to make them more usable.

Bobbie: So, usability being this really key element in the center. We hear a lot about the humans either being the weakest link or the greatest innovation in situations. Do you see security and privacy coming together? Being separate? Are there use cases where they are one or the other?

Lorrie: I think security, privacy, and usability are often in tension with each other. All three of those things, I think, can be in tension, but they don't necessarily have to be. It is great when we can find ways for them to work together, where the most secure thing we can make is also the easiest thing, so that users don't have to decide, *Do I want convenience, or do I want security?*

Bobbie: Are there good examples of that that you have really been able to push over the last decade or so?

Lorrie: Well, I think if you look at encryption, any time we have an encryption tool that users have to do something to use, they pretty much don't use it unless they are required to at their job. But we have something like HTTPS in a web browser where the user doesn't have to do anything. It just works, and that is great. That is convenient. Now there is a limit to that, because it just works under normal circumstances. But if there is an expired certificate at a website, then the user is going to get a prompt that they are supposed to do something. It breaks down because for most users they can't really distinguish between the website forgot to renew their certificate and there is actually a man-in-the-middle attack. It is not perfect, but that is the direction that we are going in.

Bobbie: Not design it more securely but make secure use by default the more frequent choice. Are there examples of more private by default?

Lorrie: Well, I think if we look in the physical world, we can see good examples of privacy by default. So, for example, there are bathroom doors that, when you go in and lock the door, it also turns a thing to tell people that it is occupied, and you don't have to give any special signal. You don't have to hang the occupied sign. It is built into the lock. So, I think those sorts of mechanisms are really wonderful.

Bobbie: I hadn't thought about it in that context. So, how do you make people more aware of the fact that something is private or not, as it is executing, as well, so they can make decisions as a part of it. I like that.

I think today about this idea of data, and data being so pervasive. We are leaving—what do they call it—digital dust, with us everywhere we go, and it is being monetized in some way or another. How do you see that affecting the economics of security and privacy?

Lorrie: People often say that all these free services that we get, basically, we are the product. The reason it is free is because we are being monetized. So, there are a lot of business models that are built on collecting our digital dust and monetizing that. That is a case where when people find out about it, they often don't like that. They don't want to be tracked in that way. We do have a tension between wanting these great, convenient services and not really wanting to be tracked to that extent.

Bobbie: I always worry about the click bait, right? Participate in this competition or in this thing. It feels like it's just an opportunity for us to feed some monolithic infrastructure that can then use that information in some way.

Lorrie: Yes, definitely.

Bobbie: It is interesting. I have been thinking a lot lately about aesthetics and how aesthetics is key to usability. This is actually a place where you and I have a little bit in common in addition to our professional lives in that I sew and quilt. I know you do as well. It has been fun to think about how these things come together, and I know you have brought them together in your career. How do you think about aesthetics and how it feeds your work in privacy and security?

Lorrie: I definitely think about aesthetics a lot in my work. I had an opportunity several years ago to actually take a sabbatical, and I spent my sabbatical at the art school here at Carnegie Mellon. I had to tell the dean what I was going to do on my sabbatical. I said, *Well, I'm going to visualize security and privacy through art*. I wrote like all of one paragraph, and it was approved. So, I went over to the art school with my sewing machine and lots of fabric and just started sewing things. Then, part way through I said, *Oh, right. I was supposed to do something related to security and privacy*. So, I started thinking about how I could incorporate security and privacy into my artwork. One of the obvious things, since I was making quilts, was that I needed to make a security blanket.

Bobbie: I like the entendre there.

Lorrie: Then the question is, *What does the security blanket look like?* What I ended up doing, because I was doing work on passwords, was I did a visualization of bad passwords. It is a big word cloud. It is done in colors like a baby blanket, so, it is like this security blanket, but it actually offers no security. That was one of the projects that I did. I also did some related to de-identification and privacy that were kind of interesting. I also made a password dress to go with the password quilt. It was a lot of fun. That was where I explicitly was working on security and privacy with art.

One of the things that came out of that was actually collaborating with some of the faculty in the art school. We did a project for Women in Art and Cybersecurity, which I got to participate in. We had about a dozen female artists and technologists working together for a week. We each had a project that got put together into a book. My project was called Privacy Illustrated. I went around and collected drawings of privacy. So, I started with kindergartners, and I went into a kindergarten classroom, and I asked the kindergartners to draw pictures of privacy, which was fascinating.

Bobbie: What did they draw?

Lorrie: A lot of potties.

Bobbie: OK, I can see that.

Lorrie: But also, clubhouses, trying to hide from their siblings. When you are in kindergarten, a big privacy threat is actually your brother or sister. Then I went into elementary schools, and I saw similar types of things, and then high school, and then adults. The older they got, the more we started seeing technology coming in. Things that were in the news, the NSA started becoming part of it. I actually saw potties in every age group, a very common theme. But yes, that was really fascinating.

Bobbie: How did that then inform what you are taking on in your research?

Lorrie: We collected, at this point, over 400 of these drawings. We have a website that they are on. A couple of years ago, my Ph.D. students said, *Can we systematically go through these drawings and learn something?* So, they went through and basically coded each drawing as to what was depicted in the drawing. They also looked at some of the privacy frameworks in the literature. They looked to see which of the elements in these privacy frameworks were represented in the drawings and which ones did we not see in the drawings.

It was a really interesting exercise in seeing kind of how people think about privacy, with the caveat that there may be some things that they think about that they don't draw, because they can't figure out how to draw. We don't [know] if they are not thinking about them, or they just couldn't draw it, but it was still very interesting. We actually wrote a paper that was presented at the Privacy-Enhancing Technology Symposium.

Bobbie: I would imagine that showed things where the frameworks were actually addressing a different privacy concern than what these individuals might have thought about.

Lorrie: We saw that there were things that experts talk a lot about. For example, how we control privacy settings. We saw some of that in the drawings, but that wasn't as in the forefront as it is in expert conversations.

Bobbie: We talk a lot in the security community about whether security and innovation is a false choice, right? Security is oftentimes seen as being the anathema of innovation. Are security, usability, and privacy—even though they are in tension with each other—is it really a false choice? Can we not find a balance between the three?

Lorrie: I think, in some cases, we can find a balance. Sometimes we have to be more creative to figure out how to do that. We recently had privacy regulation in a number of jurisdictions, and there is talk of additional privacy regulation. We hear from companies sometimes that these types of regulations will hurt their business. In the short term, they are probably right, but in the long term, I think we should really think about it as an opportunity to come up with new business models that will actually benefit people and not just feed off of invading their privacy.

Bobbie: It strikes me that so much focus in the regulations has been on trying to create transparency about what the privacy rules are that a particular service is operating under. Are you seeing that making a difference?

Lorrie: I think it makes a little bit of a difference, but not as much as we would like. I have actually been working in this area for over 20 years. I was involved in a W3C privacy standard, which we started work on it in the late 1990s. The idea was to take website privacy policies and put them in XML, and then your web browser can read them automatically, so you don't have to. The thought at the time was this would be really convenient for consumers. It would encourage websites to have better privacy policies, once people were actually looking at them, or their browser was looking at them. It was a great idea. It never really got adopted. It is a standard, but it has now been demoted as the standard. No one is using it. It is disappointing that that wasn't more successful. Ever since then, people keep suggesting that again. People will say to me, *I have this great idea. If we just took privacy policies and made them computer readable*! I am like, *Yeah, yeah, we tried that*. But I think it was a good idea. It is still a good idea, and I think there is increasing appetite to actually being able to do that. Only what we need now is kind of the idea we had before but now on steroids. In that it is not just websites that are collecting our data; it is all of these devices in our environment. Nobody has the time or patience or interest to go and interrogate every smart lightbulb they walk by to find out what data they are collecting. So, we really do need those computer-readable policies. Then, we need user agents that can consume that data and configure our settings for us based on one set of preferences we provided early on.

Bobbie: Perhaps this is the tie back to aesthetics again, right? You need the computer-readable and presentable in a way that is clear and understandable to the person walking by, right?

Lorrie: Exactly. Most of the time the person walking by is not going to want to see it. But if today I say, *Well, actually, I do want to know what is going on in here*. I should be able to look at my device and have some understandable representation of what is going on. That is the kind of work that my students are working on right now, trying to design *what does that information look like?* We are also working on designing what we are calling a privacy and security nutrition label for IoT devices. We are looking at, on the package of those smart devices, can we put some really understandable information about security and privacy?

Bobbie: Some of the work we are doing is on bills of material. So, very related in the context of, it isn't clear what the components of those devices are. Without knowing what those components are, you don't always understand the kinds of risks you are accepting by bringing even that macro-device into your environment. So, I can see linkages between these two.

Lorrie: Yes, they are. In fact, we have designed our label to be two layers. The first layer would be on the box or on the website. Then there would be a link or a QR code to the detailed layer. In the detailed layer, if there is a bill of materials, there would be a link to where you would get that as well as a bunch of other things that are technical details that most consumers aren't interested in, but the experts, and, in an enterprise, the people who may be making those purchase decisions, would want to see. We want to link all of that together.

Bobbie: And, as you define the label, it strikes me that back to the making it available by default becomes important. *How do we bring this into the development process, so the production of the content of that label happens by default, since there is so much instrumentation now in all of the development and production processes?* I can see a future different than the past with this activity.

I would like to explore something a little bit different. I heard once someone say that we always grossly overestimate what can be done in 5 years and underestimate what can be done in 10. So, what problem did you expect that we would have solved by now that we are still tackling?

Lorrie: With the whole experience with P3P computer-readable privacy policies I thought that… It was easy. There is nothing too technically sophisticated about that. Had you asked me 20 years ago whether we'd still be trying to figure out how to get these things adopted in 20 years, I would've said, *No-no, that's the easy part.* But it turned out, actually, the technology was the easy part. Getting it adopted was not easy at all.

Bobbie: Yes, back to the humans. So, what have we solved that you didn't think we could? What is the converse of that one?

Lorrie: I think we have made a lot more progress on automating things than I thought we would. Self-driving cars actually really surprised me. We are not 100 percent there yet with them, but I would not have predicted we would be as far along as we are.

Bobbie: I have to say, I thought you were going to say that you would have thought we would have been past passwords by now. I love the fact that you went someplace different. I keep thinking with as much drama as we been through with passwords, I would have hoped we would have found a different authentication mechanism by now that has been adopted.

Lorrie: Well, too many people have predicted the death of passwords, including Bill Gates, and been wrong. So, I am not going to go there.

Bobbie: Not touching that one. Yes, that makes sense.

We touched on autonomous vehicles a little bit. I know here at Carnegie Mellon, we are doing a lot with robotics and artificial intelligence [AI]. What are the most pressing of the privacy and security challenges in that space?

Lorrie: I think there are just tons of them. I think there are both challenges and opportunities with automation and AI and security and privacy. I think that there are a lot of vulnerabilities that can be exploited using machine learning approaches, but we can also use them to defend things as well. On the security side, a lot of it is about vulnerability, exploitation, and defenses, but on the privacy side, I think there becomes issues of fairness and equity and things like that. Because as we automate decision making, we end up inadvertently baking biases into the system that we don’t even realize that we are doing.

Bobbie: So, a lot we have to watch out for, right. I think, to some extent, the design patterns we have used in the past break a bit in this space. So, we really have to think about new design patterns here in order to treat data as the first-class citizen that it is in the space that is here and to recognize all of the data that we have as the manifestation of all the decisions we have made in the past with all the biases that we have brought to those decisions. I can see a rich future there. So, you are not going to predict the death of passwords. Any thoughts on what the next most pressing problem might be?

Lorrie: I don’t have a good prediction on what is pressing. I think in general it is really defending our systems from attacks of all kinds. I think as we have more technology in the hands of more people, it is offering great services and convenience, but all of these are new attack vectors. I think there is a big rush to get new products to the market, and I don’t think security is the first thing that they are thinking about.

A lot of the startups are really not thinking about it at all. Now we have lots of devices in homes and people that say, *How is anybody going to, you know, cause any problems with a light bulb in my house*? But, actually, they can.

Bobbie: I think about the Miria bot, and the proof point of being able to cause problems with things that you had predicted, right? Baby monitors.

It is really interesting because I describe the security problem as one where we are always facing that adversary action of the future, but we haven't stopped facing the adversary action of the past. We live in the past, present, and future simultaneously in this connected world and have to find a way to manage our way through all of it. Last question. What's your favorite part of your job right now?

Lorrie: My favorite part of my job? I think it is working with students. I love the energy and creativity that students bring, and the fact that they come up with ideas that I would never have come up with and never thought to do. They are not always good ideas, but they come up with enough of them that some of them stick. I really enjoy working with the students.

Bobbie: That is a wonderful impact on seeing a future that is going to be different from the past because of their creativity. So, I like it. Thank you so much for coming and talking to me today. I really appreciate it, and the collaboration between our two institutes is really wonderful. So, thank you.

Lorrie: You are welcome.

Bobbie: If you would like to learn more about CyLab's research, please go see their website. The URL is presented at the bottom of this screen. If you like to see more about what we are doing at the Software Engineering Institute, please visit our website and see the work that we are doing for the Defense Department and [to make] the Internet [more secure]. Thank you very much.

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. Thank you.