"We created a zero-day at the time for a particular manufacturers and ICS system. And what we figured out was really like an HMI type of interface hack. We could make it look like the prison doors were closed to the prison guard who is monitoring the whole system when, in fact, we had opened everything, even straight out to the gates out to the public roads and everything was on this system."

MARCH 16, 2020

Prison Breaking the System

Presenter: Tiffany Strauchs Rad

Summary

An effective way to learn how to fix things in cybersecurity is to practice breaking them – once you've done that, you're halfway there. Tiffany Strauchs Rad, CEO & Co-Founder of Anatrope, Inc. learned security skills like lock-picking and social engineering from her father, a former CIA agent and writer of the film *Sneakers*. She discusses her experience constructing a prison break zero-day, vulnerability research, and more.

Transcript

Brian Contos:

Welcome to the Cybersecurity Effectiveness Podcast, sponsored by Verodin. The Verodin Security Instrumentation Platform is the only business platform for security that helps you manage, measure, improve, and communicate security effectiveness. I'm your host, Brian Contos, and we've got a really special guest today. Joining me is Tiffany Strauchs Rad. Welcome to the podcast, Tiffany.

Tiffany Strauchs Rad:

Hi. Thank you for having me.

Brian Contos:

So, Tiffany, there's a lot I want to discuss with you, but before we get going, you have such a deep and interesting background. I was hoping you could give everybody a little bit of background about you and the path that you took that led you to a cyber and what you do today.

Tiffany Strauchs Rad:

Okay, great. I have a little bit of an unusual background that led me to cyber, but right now I am the CEO and co-founder of Anatrope. I do wireless automotive technologies and security and data analytics. So, I look at signals that are being emanated from vehicles, trucks, things like that. I'm also an adjunct professor in the Computer Science department at The University of Maine, their Portland campus. And I've been teaching there for going-on 15 years.

Tiffany Strauchs Rad:

And I've recently joined the faculty as an adjunct professor at UC Berkeley, which is in their master's program of Information and Cyber Security.

Tiffany Strauchs Rad:

I have a background of working for large IT companies and also for defense contractors doing everything from industrial control system research to reverse engineering components in vehicles and systems operations. So, like open source intelligence work for a large IT company.

Brian Contos:

Very cool. And one of the things that I thought was really interesting when we first started talking, and by the way, congratulations on the UC Berkeley bit before I forget about that. That's absolutely awesome. Is that your focus is actually on the research side and you're steeped pretty heavily in that. What was the allure? What really drove you into the research end of things?

Tiffany Strauchs Rad:

Well, I grew up in Great Falls, Virginia, which is right next to McLean, Virginia, where one of the big government agencies exists.

Tiffany Strauchs Rad:

My father was a Clandestine Agent with the CIA for a while. I don't know how long, but I grew up in that kind of atmosphere where my dad was doing very interesting work and at times would bring home some projects and we kind of get to see what he was working on. He had a lock pick set that was the biggest still to this date I have ever seen. So, I learned a lot about why he was learning how to break into places so he could make places more secure so other people can't break in.

Tiffany Strauchs Rad:

So, after he left the agency, sometime I think in the late 70s, early 80s, he started his own company. And as far as I know, he may have been one of the very first security practitioners. And this was what he was hired to do, was red

team things, places in particular. He'd do it through [what] we now call social engineering – he just called it acting. That's what he did for the agency and got a background in that as well in a way.

Tiffany Strauchs Rad:

But he was learning how things didn't work. Like for instance, x-ray machines and airports. He'd have one in his office and he'd be learning how you could send the various things through without someone who's trained reading the monitor to be able to determine what is going through the x-ray machines.

Tiffany Strauchs Rad:

So, when he figured out these things, he not only used it for red team projects that he was hired to do, but he also helped design better security standards. His background was in Electrical Engineering, so he focused a lot on the circuit design of how cameras and other types of sensors could be built and how he could design them better. So that's how I started out in the security industry, was working with my dad.

Brian Contos:

That's such a cool background. And your dad's time with the CIA and he was also a co-writer for the movie Sneakers, is that right?

Tiffany Strauchs Rad:

Yes. For many years. Actually, most of my young years that I recall my dad was in our basement working on a screenplay. Him and others wrote Sneakers. It was shelved like three or four times before they finally found the cast that became what we all know -- I think it was in 1990 -- to release a movie, Sneakers.

Brian Contos:

Yes, Dan Aykroyd and Robert Redford and yeah.

Tiffany Strauchs Rad:

Yeah. It was really cool to be able to go to the premiere of that and knowing that my dad wrote a lot of the sneaks in it. That's what he called it and that's why it's called "Sneakers." He snuck into places and it was interesting watching him develop that film.

Tiffany Strauchs Rad:

And what a lot of people know now is he actually wrote some technical inaccuracies into the movie and two years ago at DEFCON for the first time ever, we were on stage and he talked about all of the places where he designed this wrong in a way that if you tried it to copy the film to break into a bank or whatever, you'd get caught because it was incorrect.

Tiffany Strauchs Rad:

He didn't want to make a training video for criminals. And actually, at that time, the movie production studio, it didn't hide either. They didn't want the realism of it. And it worked pretty well. So, for a lot of years, no one knew until two years ago at DEFCON, he gave a presentation on here's how you'd really do it.

Brian Contos:

Now do you see your dad as more of the Dan Aykroyd or the Robert Redford character in that movie?

Tiffany Strauchs Rad:

Actually, his character is a cross between two. Sydney Poitier's character, the former CIA agent, and also Robert Redford, the guy who started the company and that character Carl is based on my brother Carl, let's put it that way.

Tiffany Strauchs Rad:

So, my dad wrote a lot of things into the movie that were the type of work he did at his company. Because at that time that type of Red Team company was very unique.

Brian Contos:

Yeah, that's really interesting. What a cool background. Well, that answers my question of how you got into this space pretty easily – "I was born into it."

Tiffany Strauchs Rad:

Yeah. I knew how to pick locks from a really early age.

Brian Contos:

That's awesome. So, let's talk a little bit about DEFCON kind of Black Hat. They're behind us now. So, you've given some talks in the past, haven't you?

Tiffany Strauchs Rad:

I have, yes. I've given two talks at Black Hat and five at DEFCON and I've given presentations on everything from the legal aspects of hacking to the digital millennium copyright, right at issues with security research, computer fraud and abuse act.

Tiffany Strauchs Rad:

And then I also have given technical presentations about some security research I've done. Because I'm also a practicing attorney in addition to teaching and working in the security space.

Brian Contos:

You just need to keep on adding hats to that, don't you, Tiffany? What an underachiever.

Brian Contos:

Let's actually dive down into a prison break a little bit. I wanted to talk about that. And, of course, that's it and you can give the audience a little bit more background but of course that's the industrial control system, SCADA based attack. But I was hoping you could give us a little background on prison break.

Tiffany Strauchs Rad:

Sure. So, one summer, DEFCON submissions were coming up and I had this idea. At the time there hadn't been a lot of industrial control system and SCADA research given at either Black Hat or DEFCON. But that summer, actually my friend Dillon Beresford was going to be giving a presentation about the potential for vulnerabilities and exploits to break gas pipelines. And I didn't know about his presentation until actually the federal government told me when we did our responsible disclosure at CIA headquarters. Which was a fantastic invitation to do a disclosure.

Tiffany Strauchs Rad:

I was thinking I knew these devices were in a lot of things related to automotive, so in the automobile manufacturing plants on some things they control communications for instance, like the network on planes, and I'm like, "Where else is it?" Because we're not going to be able to hack a plane. I don't think at this point we have the accessibility to do that.

Tiffany Strauchs Rad:

But could we build a prison and essentially mock something up in our basement of what the computer systems would look like? What would happen if we could create an exploit for that in a safe sandbox environment? Could we do it?

Tiffany Strauchs Rad:

So, a team of four of us in two weeks created a Zero-day at the time for a particular manufacturers and ICS system. And what we figured out was really like an HMI type of interface hack. We could make it look like the prison doors were closed to the prison guard who is monitoring the whole system when, in fact, we had opened everything, even straight out to the gates out to the public roads and everything was on this system.

Tiffany Strauchs Rad:

Even we found out later to do hot water in the prison. How long the hot water is distributed. That's also Industrial Control System type, controlled by that.

Tiffany Strauchs Rad:

So, there was so much we learned as we went along too, because one of the members of the team was in fact my father and my father had done a lot of design work more for the physical and electronic security systems. So, he knew when I asked him like, "Hey, is this particular manufacturer's device in prisons?" He's like, "Just about all of them." And I'm like, "How often do they update that?" He's like, "Just about never."

Brian Contos:

Yeah.

Tiffany Strauchs Rad:

So, he knew how the prisons were situated. So, when we gave our presentation, we gave a presentation about the layout of a prison, how many control points are on each door and why the ICS, Industrial Control Systems were used for prisons. So many doors, so many points on it. I think there were 125 individual points being monitored on each door to a cell.

Tiffany Strauchs Rad:

And so, we did this and the Zero-day worked pretty well. One morning, not long before DEFCON, I got a call from the FBI's director for the cyber security division and they wanted us to give a presentation and we are invited to CIA headquarters to do it. So, I'm like, this is our great chance to do our responsible disclosure and to tell them also we are not releasing this Zero-day to anyone. It's not for sale. If someone else wants to replicate our research, they can go ahead and do it, but we're not going to release it because we knew that there were a lot of safety concerns that we had. Should this Zero-day be issued.

Tiffany Strauchs Rad:

Because as we'd seen in the past, manufacturers had not issued patches quickly, so we weren't going to go full disclosure at DEFCON. So, we went to headquarters, we gave our presentation and we got to see after the meeting Cryptos. I was pretty excited to see that. We got a tour of the real Spy Museum, which is actually in the old building for CIA headquarters. When you go to DC you see the Spy Museum, but some of those are replicas. Not all, but some. Some of the real stuff, it's there.

Tiffany Strauchs Rad:

So, we got to see it. My dad's like, "Oh, I remember when I had this kind of kit and this is the kind of disguise I'd use that that looks just like it." And it was really cool to get a tour. We had a tour guide and my dad giving a tour of the real museum and Crypto obviously was fantastic to see

Brian Contos:

What an amazing experience. I'm wondering because, you're a practicing attorney and clearly you have this very technical background as well. Something that not a lot of people possess both sides of that. When you're doing this research into Zero-days and digital weapons, from a market perspective, what did you learn? What was that like?

Tiffany Strauchs Rad:

Well, one thing that I did for our research and I've done for companies I worked for subsequently was, I made sure that we didn't crack or break anything. So, we didn't have any CFA triggers. I didn't have any copyright, the DMCA type of issues. So, we're straight up, we're using the software as it was designed to be used and we just found a way to exploit it, but no crack or anything like that.

Tiffany Strauchs Rad:

So, I have advised companies and other security researchers on how to structure your research so that you're in the clear, should you go to DEFCON or Black Hat. So, you don't have to worry about this. Now some people do have exploits that have done that and it's still important to know, but this is part of what I learned teaching at the university. About every two years, I have a student who has a final project that finds a pretty significant vulnerability or creates an exploit that's really a big deal.

Tiffany Strauchs Rad:

And we go through the process of disclosure to the vendor, but we also learn about the legal aspects of it that they don't have to do that. It gives the vendors some heads up that this is coming up. For some of my students, not all, but they didn't present at DEFCON, they just wanted to give it to the vendor, but anonymously.

Tiffany Strauchs Rad:

And I've learned through these processes too that this can be difficult to do, is to be anonymous. So sometimes you've got to find someone who acts as like a middleman and attorneys are good for that because we get to protect our clients with attorney client privilege. Because also I've of the research I've done, I know what this is like, I contacted a company and said, "Hey, I have a client who wants to just give this to you. So, what you do with it is up to you, but they just don't want to be named or known. So, any questions you contact only me."

Tiffany Strauchs Rad:

So, some researchers want to know that work's being done. So, they go through some of the government programs that they have, especially, there's one for US ICS Cert and they go through that and then they can see actually what the vendor's working on and they work on a disclosure date.

Tiffany Strauchs Rad:

I've learned a lot through my own research and through working with others too about the process of disclosure. But when it really came down to when we had a Zero-day, how to handle that, we all thought about and talked about the responsibilities for what we had and that's why we agreed it would never be on the internet. It was only on our lab at the time.

Tiffany Strauchs Rad:

So, this is what I learned from that and that was an interesting experience going through it myself in addition to before and later helping researchers go through that too.

Brian Contos:

It's really interesting, this process, and you get to touch the academic side of things as well. Can we dive down a little bit more into what exactly it is you do today? Because you talked about signals being emitted from automobiles and a little bit about IOT, but what's really your primary focus right now?

Tiffany Strauchs Rad:

Right now, my focus is with my startup. I analyze signals that are emanated from vehicles and every vehicle has a unique signal. And some of these are in the public spectrum as well. They're not all through cellular connections, things like that, that are more considered to be in privacy, a lot of private.

Tiffany Strauchs Rad:

But I take a look at the bunch of these signals and in the past, I had done work on reverse engineering. Like, okay, these are the signals emanating. How would you remotely get access to a vehicle? And if you could do that, what could you do? Could you control steering? Could you affect the braking? So, I learned a lot by, kind of like what I learned from my dad about how to take things apart, how to break them, and then learning about how can we learn about what signals are being emanated and what we can do about that.

Tiffany Strauchs Rad:

Right now, I consider a lot of these devices to IOT. When you get into your car, you got your phone, maybe everyone else in your car has their phone too. And a lot of these things are bumping up against, like for instance, beacons when you're in a big city.

Tiffany Strauchs Rad:

And soon we're going to have the vehicle to the roadside unit and then your phone is connected to your vehicle, could that be connected to the roadside unit. How much can be known about the driver. And we're right now at this point with the design of the infrastructure of smart cities where we need to start to think about, well, not to start to think about this is going on now. Security and privacy because the industry has learned, you don't add this on at the end. That's a mistake, you design things in.

Tiffany Strauchs Rad:

So, a lot of us want convenience when we are out and about doing stuff. I have some students who are very privacy conscious. They don't use Google ever. They don't use Google Waze. They use old school maps to get places. But a lot of us today, and I think the next generation coming up too, they want the convenience. So, there might be a bit of a tradeoff that as long as the consumer is onboard with, okay, I'll give up some of this thing that's considered private, maybe use for data analytics. And in turn I get these convenience features. Like, I can order pizza while I'm driving home and it'll be there and when I get there, stuff like that.

Tiffany Strauchs Rad:

So, all these technologies are being designed and right now I'm working to design this type of stuff in. So, this is one of the things that I do right now is looking at personal and public transportation, how our vehicles connect with smart cities and the infrastructure, like the grid in particular.

Tiffany Strauchs Rad:

And I love the analogy, the grid because that's really what it's like. There's so many data points. It is actually so interesting. And for me, I love tracking and looking at patterns and the value in what is the data analytics industry and it's growing so quickly and it's very interesting and valuable.

Tiffany Strauchs Rad:

So, that's part of what I'm doing now too, is seeing what we can do to give the convenience and look at the data, but also making sure that privacy consciousness is designed into the products and security.

Brian Contos:

Yeah, it's so great to hear there's people like you working on the problem of designing in as opposed to retrofitting and bolting it on later because you're absolutely right. We've proven time and time again and hopefully we've learned that it just doesn't work and there's such a gap between getting it fixed after the fact. That's fantastic.

Brian Contos:

Tiffany, as we wrap things up here, there's a question I like to ask everybody on our show and that's who's your favorite superhero or supervillain and why?

Tiffany Strauchs Rad:

Tony Stark is my favorite superhero and has been since the very first Iron Man.

Brian Contos:

That's awesome. Well, he started it all and I don't think there can be another Tony Stark.

Tiffany Strauchs Rad:

I know. And actually, how it's wrapped up with him is disappointing to me. And what I liked about Tony Stark is I am not a Tony Stark. I'd love to believe that I'm this crazy genius that can build an iron man. But I actually really like sitting in my basement with no type of constraints and just building stuff or taking things apart and learning how they work and then building something better or different. And that's the essence of hacking, right?

Tiffany Strauchs Rad:

So, Tony Stark is a hacker and I've always loved the work that he did and he also does a lot with vehicles. He has a lot of awesome cars. I am a big fan of fast cars and I haven't had an opportunity yet to hack one and take one apart. Like, if anyone wants to give me a McLaren, I'd be very happy to do a contest on one, but you may not get it back without the warranty voided. But, that's why I really enjoyed those movies with that particular superhero. He builds stuff and he's not a superhero, like any magical powers. He just is interested in stuff and builds it. So that's why I respect that one.

Brian Contos:

Right. That's awesome. I think one of my favorite scenes was from Iron Man 1, where the antagonist in the movie has all these engineers trying to build the Iron Man suit and the power core that he was using. And they're like, "Tony Stark built this in a cave with a box of spare parts." And they're like, "We're not Tony Stark." That's awesome.

Tiffany Strauchs Rad:

Yeah, it’s great.

Brian Contos:

Well, Tiffany, thanks so much and thanks to our listeners for joining. Be sure to check out other Cybersecurity Effectiveness Podcasts, sponsored by Verodin.