Barclay Damon Live Presents *Cyber Sip™*
Season 3, Episode 7: "Keeping Hackers at Bay: The Role of an Ethical Hacker" With Ziming Zhao

Host: **Kevin Szczepanski**, Barclay Damon

[Kevin Szczepanski]: Hey, everyone. And welcome back to Cyber Sip. Joining us today is Professor Ziming Zhao, who is an assistant professor in the Department of Computer Science and Engineering at the University at Buffalo. Professor Zhao also directs the Cyberspace Security and Forensics Lab, otherwise known as CactiLab. And his research interests are . . . Why don't I ask you? Professor Zhao, what are your research foci?

[Ziming Zhao]: Thank you, Kevin, for having me. Yeah. I basically work on all kinds of cybersecurity problems. Sometimes go beyond cybersecurity and go to the physical security world as well. So my main focus right now, my lab, we mainly do systems and software security. We are particularly interested in all kinds of IOT and embedded systems because those systems, they were deeply embedded before ten years ago, no one worried about their security. But now those devices are connected to the internet as they are facing all kinds of attacks. So, however, their hardware is different from our cloud or desktop computers. Their hardware do not provide all the security features those systems. So how do we secure the software and OS on those systems? That's one of our research focus.

[Kevin]: Yes. Well, you're at the forefront of cyber hygiene and I'm really excited to have you here today.

[Ziming]: Thank you.

[Kevin]: We're going to talk about ethical hacking in the time we have. And so I guess the first question I should ask you is what is "ethical hacking" and is there such a thing? Can there be such a thing as ethical hacking?

[Ziming]: Sure, it is definitely a thing. To me, I think ethical hacking is a hacking in an ethical way. What it means is... the goal of ethical hacking is not to identify the vulnerability as for profit, not to exploit for profit or not even do that for fun, but to responsibly disclose the vulnerability to the vendor and to help them fix the vulnerability before they are exploited to by our real-world adversaries or cyber criminals.

[Kevin]: So why then, would anyone want to be an ethical hacker?

[Ziming]: Well, first of all, I would say hacking itself is very fun and it's a legal way to be a hacker, right? Hacking is fun. It's challenging. So I teach software security at UB, and I have a capture the flag platform which I developed to hundreds of challenges and to the students. I have been offering that course for many years and the students love it because they told me it's like brainteasers. Brainteasers keep you young, right?

[Kevin]: Yeah, they do.

[Ziming]: Yes. And I will say it is a very early stage of software and system hacking like back in the '80s, you know, was mainly for fun. It was all really for profit because at that time there were not many cyber criminals.

There are just some people really good at systems and the figure out all of this can be exploited this way. So and I feel like it’s in our human nature that we want to break things. We want to find the vulnerabilities. We want to break new ways that no one did before. Right. So it’s not necessarily malicious to do that. Right. It’s like we enjoy building Legos. We also enjoy breaking Legos at the same time.

[Kevin]: I remember that.

[Ziming]: Yeah. So it’s not necessarily malicious, and ethical hacking is the way to enjoy that kind of fun but also doing a legal way.

[Kevin]: Right. So a professor who needs an ethical hacker and why? And… there’s got to be there’s something more than just curiosity and the fun of breaking things which by the way, I’m remembering I did love to do. I would build these large Lego ships and then I would smash them apart. And they never went back together the same way.

[Ziming]: Yeah. If you go to children’s museum every day, know kids doing that well, yeah, right. So. So who needs a hacker? I would say whoever may be attracted by cyber criminals, they should have ethical hackers try to find the vulnerabilities before the criminals find that. Our society as a whole, we need ethical hacking because security is an arms race. There is no such thing as absolute security, secure. I know many companies out there advertise how our product is unhackable. That’s just that’s to me, that’s a fraud.

[Kevin]: To me, it’s an invitation to be hacked. Yes.

[Ziming]: Yes. So that’s like the Art of War says that you need to know yourself. You need to know your enemy so you can win the war right? So if the defenders they don’t know how attacks work, there’s no way they can come up with effective defense. Actually, what I feel is that if the defenders do not really know how attacks work, they don’t even have the motivation to come up with good defense. So like, for example, in my software security course, we do not only teach how to exploit vulnerabilities, we also teach the state of art solutions to defeat those attacks. However, we always teach attack first. If we just teach them defense, the students that do not understand why I’m learning this, what’s the motivation? And this is something very hands on. You have to do it. You have to feel it. For example, every year I force my year one, year two PhD students to participate, seek a particular CTF called Embedded CTF, and in that CTF the students were develop and design a secure system for two months, then gave that system to other usually college teams to hack each other.

[Kevin]: Right.

[Ziming]: And you can imagine that after the two models, after development and design everyone’s confidence level is super high. They feel, I designed such a secure system, right. Then three years ago that that version of that competition or our system was online for two hours, then got hacked by two universities. Then my students was like, Oh my God, security is so brutal. And for me, as a professor, there’s no better way to teach my students. Security is brutal like that, right? It’s an arms race. And so go back to that question who needs an ethical a hacker? And that’s why I believe the society needs that. Many companies needs that. And but I want to bring up something else as well, is like even if the companies, all the organizations, they were indeed ethical hackers, but they also need to know that ethical hacking or pen testing is a badness meter. It doesn’t tell you how secure your system is. So this is not said by me. This is said by Gary McGraw. So he was a pioneer in software security back in the ’80s, ‘90s. He has several books in software security before. Most of us know how to do buffer overflow. So the badness meter means that it’s the pen testing finds many vulnerabilities in your system. It means your system is so insecure and you should fix that. However, even if the pen testing doesn’t find any vulnerability, it doesn’t mean your system is secure. It only means that pen testers or ethical hackers do not know how to hack your system right from else. Someone else out there may know that. Right? So it doesn’t mean it’s unhackable. Right? So I think that’s equally important that one when people, companies, organizations they hire ethical hackers to find vulnerabilities. They should also have that mindset. Of course, they can raise the bar, can make it harder to hack, but it doesn't really mean your system will be unhackable. Yeah.

[Kevin]: Right. It's logic, right? Yes. If there's no penetration, it doesn't mean your system is safe. It just means that the hacker was unable to penetrate.

[Ziming]: Yeah. Exactly, we don't know what we don't know. Right.

[Kevin]: Right, right. It's a known unknown.

[Ziming]: Yes.

[Kevin]: So what I'm hearing, professor, is you've got to be able to hack in order to be able to defend.

[Ziming]: Exactly.

[Kevin]: And the better the hacker you are, the stronger the cyber defense you can build to a particular network or system.

[Ziming]: Yeah.

[Kevin]: So. All right, so I'm an organization, and I just. I need pen testing. I need some ethical hacking. Tell us how that works. I mean, I take it ...I know some do this, but you don't just hack into some network randomly and then pick up the phone and say, hey, we hacked in, we'd like to help you. How do you set about to arrange with a client or a customer to engage in ethical hacking?

[Ziming]: So I want to say most of companies right now, like the bigger ones. They have their own ethical hacking thing. They probably do not quite that way. Right. They their security operations center, their SOC may have some reporting. They're not just analyzing incoming traffic, but also try to find out vulnerabilities of their system themself. And also many companies they have they have all kinds of bug bounty programs, rewarding programs to help, like some individuals... ethical hacker individually to get some kind of a reward by reporting the bugs. And also there are many hacking competitions. Big companies also organize that to hack their real-world system. Also there are hacker platforms right now. Companies try to have to something like a third-party platform just to collect ethical hackers with companies in need. Um, I see there are all kinds of business model right now going on. I'm not sure because I'm not in the business world. I don't know where this is going. Yeah, Yeah.

[Kevin]: So do you, Professor. You mentioned bug bounty programs. I want to get your take on that before we move on, because from what I understand, some are better than others. There are hackers I know that have reported on their ability to hack into certain companies. And sometimes the company will say, oh, thank you very much. Yes, our bug bounty program. Sometimes the company will threaten the hacker with criminal prosecution for having done something unlawful.

[Ziming]: Yeah.

[Kevin]: Is there a fine line between bug bounty programs and maybe unethical hacking? How does that work? How safe is that for an ethical hacker to participate in?

[Ziming]: I want to say, for obviously... things have changed dramatically in the last decade and now I would say most companies realize the importance of ethical hacking. They realize that people from most of a lot of from academia, they find a vulnerabilities. They are doing this just for science and they responsibly report it to you. And you should be grateful for that. They're not trying to exploit you. And also there are some professional hackers also trying to be ethical. Maybe at some point of their career they did something bad. But everyone trying to be a legal now, right. So, yeah, so for them, there are people live on this. There are people live on bug hunting. And I'm very happy to say that people can live on this now. They don't have to do illegal things and enjoy doing this but want to take them off. Oh, I think more and more companies, organizations will be aware of this and join this trend to award ethical hackers. And I hope that's where happen sooner than later.

[Kevin]: Right? No, I agree. And it sounds like you're really passionate about

[Ziming]: Of course. Yes.

[Kevin]: You do think is important. So I know you mentioned you're not in the private sector. You're a professor at UB. But let me ask you this and maybe you could walk us through it. Suppose you were in the private sector. You're an organization or you know, you're retained. Someone says, Professor Zhao, we really need some pen testing and we've looked into your team. We think you're the right fit and you're hired, or you're not. You're just... it's through some other program. And you do successfully hack into an organization's network force system. What happens next?

[Ziming]: So I imagine as a responsible hacker you need to clearly document what happened to why this happened. Is this like a one-time thing or as there is a guaranteed way to be successful every time you do this. Then work with organizing company to find the root cause, the problem, and to think about how to help them to fix the problem. So I think that it is what an ethical hacker can do. But for academia, it's a bit different because we are now just into vulnerabilities, right? We're more into new vulnerabilities, we're into new ways to find vulnerabilities. So we are trying to think about the scientific value, not just the real world, broader impact of any of those things. So because of that, I think our focus will be a little bit different. For example, right now we are in the AI era I would say, I mean, yeah, ChatGPT, everything, large language model. Then I was thinking as a systems security software security guy, what should I do? I mean, doesn't mean I also need to do the prompt engineering. I was thinking maybe not. Maybe I should shift some of my focus from the CPU-based systems to GPO-based systems. There are a lot of similar software and system security problems, similar in the GPO systems to the CPO system, but CPO system where I've been working on for three decades, four decades. But GPO system is relatively new. Then I actually have friends that discovered something called return oriented programming on CPU. And it's not my work. My friend's work.

[Kevin]: Say that again, Professor. I want to make sure our audience gets that.

[Ziming]: Return oriented programing. So it was discovered like back in 2007, 2008 by a professor at UC San Diego. He published a paper on that. So basically it's not a code injection attack. You can reuse the code gadgets already on the computer system to hack it yourself. It's like you have a Lego of Yoda, and it's computer generated, it's secure. However, if you break it down to smaller Lego pieces, you can make a Darth Vader out of that.

[Kevin]: Mm, yeah.

[Ziming]: You can weave some malicious code out of benign code.

[Kevin]: Yes.

[Ziming]: So but it was done on CPU before, so one of my friend, his team actually recently discovered that they can do similar things on GPO-based systems. So their paper is still on the review, so I cannot talk too much about it, but...

[Kevin]: Right.

[Ziming]: That's what I'm thinking. Right. We, we need to that is also something interests academia, right, something new, something no one has done before.

[Kevin]: What's your take on the link between academia and the private sector? How is that relationship? Does the private sector pay attention to and take advantage of what academia is doing to push the science and the technology forward?

[Ziming]: Oh, well, I would say academia, industry, obviously, they go hand in hand. We need each other sometimes new . . . especially where in computer science, right? It's not like we are mathematicians. There are open problems. There ...which has been there for 200 years, 300 years, and we're trying to solve that. Well, we are still trying to solve real-world problems. And most of the problems, some of the problems they are... they only surface when we have the industry scale, those kind of user scales and we can say, oh, there is another challenge. There's another problem we need to solve. And in academia, if we do not work with industry, we will not have we do not see those kind of challenges. We cannot solve those problems. And industry, usually they are business-driven. So there... even if like big companies, they have research labs. I worked with one of the big companies' research labs before, but my feeling is still, as a companies. They have their own mission. And their own mission is not necessarily science, even if it is research-backed, that is not necessarily science oriented, right? So that's a major difference. But we do need each other. So I do not personally feel we are being taken advantage of. Well, yeah, I feel we need each other. Yeah.

[Kevin]: Yeah, I think so. Yeah. All right. I want to turn to something else, but before I do, I have a quick question for you. There is the term "ethical hacking," and then there's the term "pen testing." Is there any difference between the two or are those just synonyms, and one gets used in the private sector while one gets used in the public or in academia?

[Ziming]: I kind of feel the word "pen testing" sometimes means something more particular. It has a smaller scope. That's what I feel. So usually when we talk about pen testing, we are talking about people directly working on finding vulnerabilities. And most of those people, they are industrial researchers. They do not necessarily go very deep into academia. They use existing tools. Some of them are very good at the developer tools. But most of them are using existing tools. So their goal is more like finding as many vulnerabilities and fix them as quickly as possible, right as soon as possible and find out as many as possible. Right. "Ethical hacking" is probably... is a bigger term that can cover many other people, like people in academia. They study new ways to attack. They do not necessarily get paid to pen test a particular website or particular system. They are not necessarily into those kind of things. But as they are doing attacks, they publish papers, they show people this is possible. Right? So to me, those guys, maybe including myself, I want to we are ethical hackers, but I would not label myself as a pen tester. Yeah, in that sense.

[Kevin]: It almost sounds to me like ethical hacking employs more creativity and it's more open ended than pen testing is.

[Ziming]: I would say that... that's a much bigger scope.

[Kevin]: Yeah, Yeah. And it makes me wonder, although maybe this is we'll leave this for another episode, but I'll put it to you. If that's the case, Professor, then do we have a challenge with pen testing? Are we employing pen testing on an industry-wide basis that may be too narrow and that may need to be expanded in order to truly identify the existential vulnerabilities that an organization may have?

[Ziming]: Yes, I think a lot of the big companies are doing that. One of my PhD students who is graduating soon is talking with a major company, like a GPO company, and they are interested in GPO security. And I think, right now, the software security on GPO, probably just fewer than 50 people in the world are working on that, I think. And they are putting together a team to work on that so they are not making GPO and all those that sometimes they are thinking about how to expose the vulnerabilities. So to me that's beyond the pen testing. Obviously. That's . . . they're putting a team to do research as well in this direction. I think many other companies are also . . . Of course, this kind of things can only be affordable when the company is so big, right? So they are so mature.

[Kevin]: True. And I think it's at some point insurance plays a role and regulators play a role. We have regulators mandating pen testing, for example. And if it's... if you're regulated, you're required to do it. So that takes care of the discretionary element. But often I find myself concerned with the nondiscretionary element. You know, these organizations out there who they want to do the right thing. They want to employ all the state-of-the-art methods, but it's not affordable and it's not required. And so what do you do? How do you budget ethical hacking or pen testing into your organization?

[Ziming]: Exactly. Yeah, I would say like all the products we say in real world, probably just a very few of them has a security in design mindset right. Everyone designing anything there were think about I need to get to the market. I need to get to the user first without thinking of all of the security of that. Security always comes later. So in academia, also industry, many people have been pushing the mindset of security in design. But this has . . . I have been saying this for decades or at least a decade. People are saying that, governments also saying that, but it's not happening. I feel yeah, in the real world.

[Kevin]: Yeah, right. There are there are some, and I know many of our clients fall into this category, but it's certainly not the majority.

[Ziming]: Yeah.

[Kevin]: Organizations who are . . . who build security into every stage of the manufacturing process from design to final release and contrasted with that is what you said, which is just sort of thinking about it at the last minute. And that's I think that's going to... we're going to continue to evolve in a positive way, but we're not there yet.

[Ziming]: Yeah.

[Kevin]: All right, Professor, I know we're running short on time, but I have one other question I wanted to talk through with you. So it strikes me that the role of an ethical hacker is ever-expanding, right? Because an attack that works today may not work tomorrow. So how do you, as an ethical hacker—how do you train your team to stay up to date, on top of your game, so to speak, so that you can hack into systems as they evolve and improve?

[Ziming]: Yes. So first of all, I would say a lot of new attacks, they came out as papers, they came out as blogs, and we always follow the researchers, the best hackers, X, Twitter those other places. And we always also go to all kinds of gatherings, academia conferences. There are also conferences like Def Con where people meet and exchange ideas. And I like what you said there that an attack today may not work tomorrow. And in the last, I would say two decades, our system security improving not only on papers but also in real world. Right so back 15 years ago you'll probably remember everyone use multiple antivirus. Now we don't do that anymore, right?

[Kevin]: Yes. Yes.

[Ziming]: So attacks that work today may not work tomorrow. But on the other hand, we also say that systems that look secure today may not be secure tomorrow. Right. For example, maybe four or five years ago, we have that meltdown. We have the spectral find a vulnerability in CPUs and is also vulnerability has been there for at least 20 years, but no one knows how to . . . no one realize that's a vulnerability. And here like 20 years later, people cleverly find that, oh, we can utilize this to hack the system, right? So all of the systems that have been secure or sort of the secure for 20 years, all of a sudden they're not secure anymore. So I would say that there are multiple dimensions of this question. So yeah.

[Kevin]: Yeah, it definitely sounds like it. All right. So we're almost out of time, but I want to ask you one question.

[Ziming]: Sure.

[Kevin]: Let's say you're in front of a small to medium-sized business today and you have one minute or two to convince that organization to employ ethical hacking in order to improve its cyber hygiene. What are you going to say to that company's CEO or CISO in order to convince them that they need to do this.

[Ziming]: I will say resolve that with all the find the vulnerabilities before your attacker, cyber criminals, thus, they may put you out of business. All of a sudden. Yeah, you're done. Yeah.

[Kevin]: Yeah.

[Ziming]: So if you can't, you can think of this as an insurance. You can think this as a way to raise the bar for cyber criminals to attack your system. Yeah. So it's definitely necessary.

[Kevin]: It's pre-attack insurance. Yeah, post attack insurance can help you recover, but why not insure yourself before the attack so you don't have to recover?

[Ziming]: Yes. Yes. So like I said, having ethical hacking can definitely help you, but not necessarily. You should never think I'm absolutely secured. Right? Yeah.

[Kevin]: Right. That's how we talk about it. You can manage exposure, you can limit the exposure, but you can't eliminate it. Well, that sounds like a good place to leave it. Professor Ziming Zhao, thank you so much for joining us, was a great conversation.

[Ziming]: Thank you so much, Kevin. Thank you for having me. Oh, this is has been fun. Yeah.

[Kevin]: Oh, my goodness. It's fun for me too. And I hope you'll come back to talk. We'll talk about something new and exciting on an upcoming episode.

[Ziming]: Sure. I enjoyed doing this very much, so I hope I can come back.

[Kevin]: Definitely. Thank you, Professor. And thanks to all of you for joining us on this episode of Cyber Sip. We're back soon with another episode.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of* Barclay Damon Live *programming is the audio file. Thanks for listening.*