#CyberChats Podcast - Season 1, Episode 005 - 27 April 2023
Jessica Fitzgerald-McKay:
At the most basic level, nothing we do with our computers, be it having this zoom call or or being able to use our cell phones or being able to log in and buy something off of Amazon. None of that works without these standards being written.

00;00;18;22 - 00;00;52;14
Jen Langdon:
Hello and welcome to CyberChats, a podcast made by the National Cryptologic Foundation. I'm your host, Jen Langdon, and together we'll be demystifying the world of cybersecurity by talking with amazing cyber fanatics like you, as well as industry professionals.

In this episode, you'll hear three guests talk about their different paths to cyber. But one thing is common how they act ethically to make sure things are more secure than before.

00;00;53;13 - 00;01;23;07
Our first guest, Austen King, is a senior at Dakota University in South Dakota. And we heard about him through the U.S. Cyber Games. He'll share about how he compromises networks to make things safer. Mike Boyle and Jess Fitzgerald McKay are two special guests were hosting from the National Security Agency or NSA. They'll provide you some insight into how the values of freedom and privacy factor in when working to create the ability for a safe Internet to function.

00;01;26;02 - 00;01;44;18
Austen King:
Yeah, so kind of started out when I was in eighth grade and I got a Raspberry Pi for Christmas and it came with old books as well. My dad graduated with a degree in it and he wanted me and he always knew that like cyber was the way to go. And it's like a blossoming career field. So it's a great path for me to take.

00;01;45;00 - 00;02;05;16
So I just ran through the books. The books covered topics like Python, different hardware circuits that you could build using the Raspberry Pi, and it kind of just like expanded from there, blew up my version from that I took and I joined Civil Air Patrol, and civil patrol had a competition they competed in called Cyber Patriots. And through that, I just kept building and stacking it.

00;02;05;16 - 00;02;18;09
And then I went to cyber it because it was weeklong camp where I learned about topics from actual professors at DSU and that's where I first learned, like some of my hacking knowledge that I know today.

00;02;18;27 - 00;02;29;28
Jen:
So you've mentioned like Cyber patriot, right? You've done been involved with that. And you've attended a gen cyber camp. How have those experiences like really shaped your life?

00;02;30;24 - 00;02;52;15
Austen:

Yes, I started it was like it was basically my entire high school experience. I wasn't the most interested in the subject that they're teaching at my high school. So a lot of time I was sit there when I was because we had everyone had their own computers, so I'd spend a time in class studying computers I'd be looking at because when you use windows and that was my job, was to secure windows and have a patriot.

00;02;52;15 - 00;03;12;21
Okay. So I'd be kind of looking for ideas on what to be looking for, and I'd be like, So instead of focusing on, you know, history, which might not be the best idea, but I would focus mainly on the computer aspects of like my classroom. I'd play around windows, scrolling through all different files, trying to familiarize myself as much as possible with what was there.

00;03;12;21 - 00;03;15;28
And I'd Google a lot of things, try to learn as much as I could during that time.

00;03;16;25 - 00;03;33;26
Jen:
You're an undergraduate and you plan on doing a master's. You're a big part of U.S. cyber games. What is drawing you to also lead a cyber community club aimed at getting like middle and high schoolers in the Midwest into cyber.

00;03;34;13 - 00;03;52;27
Austen:
So I know myself, I really didn't have that way into computers. I was always tearing things apart. Since elementary school, I was always like any toy I'd have. I'd end up dismantling it at some point because I want to see how it works, right? And I didn't really have that wait to take that step into cybersecurity without that Christmas gift that I got.

00;03;53;11 - 00;03;59;16
And, you know, not everybody as parents are going to end up giving them a Christmas gift that helps them kick start their entire career.

00;03;59;21 - 00;04;05;15
Jen:
They might not. Yeah, they might not know, like, oh, I should give my kid a Raspberry Pi. That's going to be the thing. Exactly. Okay.

00;04;05;15 - 00;04;23;07
Austen:
So yeah, the goal is that we host, you know, we get outreach to schools, we get them posters, different material, and hopefully we can. The goal is not to get everyone right. The goal is if there is some student that's interested, we find that person in a classroom and we we help kick start their career or get build a new interest.

00;04;23;07 - 00;04;27;16
I didn't know they had it. And it's just a really great way to build a community together.

00;04;32;22 - 00;04;35;00

Jen:
Mike, Tell us about your path to cyber.

00;04;36;08 - 00;05;02;00
Mike Boyle:
I was a math major in college, got a master's degree in math, and then I have a good friend who was NSA and he encouraged me to apply. So I came to NSA. I was accepted. I started working there roughly 30 years ago, and I was originally doing math because we have a lot of hard math problems related to cryptography.

00;05;02;14 - 00;05;22;15
But along the way, my emphasis started shifting. I started doing looking at products that use cryptography and then started doing more and more How do the networks work that we all use to connect to things on the Internet? So I really kind of shifted out of math, although I still fall back on it from time to time.

00;05;22;28 - 00;05;48;17
Jessica:
So again, in college, I studied political science and international relations and women's studies. So these are not traditional majors for people who work at NSA. But what happened when I was in college is our nation, which came under attack on September 11th, 2001. And that made me really think about how I wanted to use what I had learned at school, particularly in science and international relations, to help.

00;05;48;17 - 00;06;16;07
I want to help. So a lot of people wanted to help after September 11th, and the government needed my help. So I, I applied along with a flood of other people my same age who I wanted to become and lend their talents. And there was a huge hiring boom also at the same time at NSA. So my resume literally says things like I took advanced math classes and I'm damn good at a crossword puzzle. That's what my application said.

00;06;16;22 - 00;06;39;00
But a lot of the skills that got me hired actually were more things like, I am good at speaking in public and I am good at understanding people's motivations because of my political science background. Like why are people doing what they're doing? And I am darn good at the crossword puzzle. So I was able to use that kind of that logic based skill set in order to get accepted into the cryptanalysis development program.

00;06;39;12 - 00;06;47;23
And that's how NSA changed. It changed. It's people who are going to be doing things like Codebreaking. So Mike was one of my mentors when I was in my intern program.

00;06;48;03 - 00;06;49;03
Jen:
Oh, that's fun.

00;06;49;27 - 00;07;15;20
Jessica:

He was getting transitioned into his work and doing things like with industry to to secure communications. And I thought to myself that that's really what I want to do. And that's really where I can use my skill set of working with the public and and understanding the politics behind how decisions get made and using that to help shape the policies we use here at UT, saying our national security systems or our computer systems that carry classified information.

00;07;16;08 - 00;07;31;20
Mike:
Yeah, I like to always kid just about the liberal arts background, but quite honestly, everything she said, That's right. She learned valuable skills. That letter actually interact with people, which is like half the battle. And also she just had an actual like problem solving skills to make sure.

00;07;37;11 - 00;07;49;27
Jen:
You also do work. You do a lot of things, Austen. You work as a pen tester, so you do computer penetration testing. For those who don't know what that abbreviation is, tell us what's involved with that sort of work.

00;07;50;18 - 00;08;11;09
Austen:
Yeah, so for I work, we pen test County. City is the state of South Dakota. So our goal is to just raise line the base level of security of all these different places. We want to make sure that because threat actors, it's getting harder and harder to go after the big targets. And I mean, you're more likely to catch the attention of the FBI if you're taking down a pipeline.

00;08;11;09 - 00;08;19;07
But if you take out, like the small counties, they might not pay the ransom. They don't really have the set up. They're not equipped to deal with those kind of things.

00;08;19;14 - 00;08;22;20
Jen:
Oh, and like defend from an attacker. I see what you're saying. Yeah.

00;08;22;28 - 00;08;44;20
Austen:
For a lot of these places, they have like nice little networks, but they don't have any security element to it. And it does not take a long time to escalate my privileges. So once I'm on the network, it might only take a few hours for me to completely compromise every computer on the network. And the goal is to just start hammering away at each of those holes that like bracelet baseline security.

00;08;44;20 - 00;09;01;11
So that way, just like it doesn't take only a few hours, our goal is to slow down if there's an attacker on the network and stuff like that. Our goal is like make sure that they know what to do if there's a third actor. I her thing is when we get caught because that means that they're looking and they're paying attention to the network.

00;09;01;11 - 00;09;02;11
That's very important.

00;09;02;24 - 00;09;18;18
Jen:
You've mentioned to me how you want to move into red teaming. What is the difference between pen testing and red teaming and what is it about red teaming that I guess speaks to your skills?

00;09;19;12 - 00;09;37;22
Austen:
So pen testing is typically seen as you're more working with the blue team. It's a very noble cause. It's you're taking steps and like just building on security, you usually don't have to worry about being too quiet because the blue team knows you're there and they're just like waving an and I just like letting you do what you have to do.

00;09;37;22 - 00;09;56;01
And just like you're you have a checklist. You're just marking everything off your list. And then like at the end of the day, you give them a report like, okay, so here's all the things we found while we were digging around. And like, it's, it's a very short it usually lasts for a test because they don't take too long as you're rolling through.

00;09;56;15 - 00;10;15;22
And it's very beneficial to have that kind of test done. It doesn't. It's cheap. That's versus red teaming is you're more testing their risk your testing the network, your testing, their response as well. Their goal is to remain under the radar. So you're hired by like one person in the then obviously you have to have a point of contact.

00;10;16;02 - 00;10;35;19
But usually they don't as much tell the team that you're starting or like the people who are supposed to be looking and your goal is to remain undetected in the network you're trying to traverse through their systems, trying to collect information, exfil. And the goal is to see if the blue team ever catches you and what you can get away with before being caught.

00;10;35;19 - 00;10;42;24
And it's just a lot more intriguing to me, like what's possible. But they're both very useful for businesses to conduct occasionally.

00;10;42;24 - 00;10;58;05
Jen:
So when thinking about like pen testing and red teaming, what are some of like ethical considerations? Because I can kind of see potentially what could happen in red teaming versus pen testing, but I'll let you respond.

00;10;58;05 - 00;11;23;25
Austen:
Ethical considerations-- just don't do either of them, particularly without permission and a contract that can get you in a handful of trouble with the computer Fraud and Abuse acts that government did say to not target good faith, good faith pen testers, or like people who are their goal is honorable of what they want to do.

00;11;24;10 - 00;11;45;17
And if they had the goal of reporting it, don't try to get them in trouble. They will tell them or they will tell the company that that's trying to like prosecute like, hey there, it was good faith like, But the company still has every right to target you and like what you did. So f considerations, just make sure you permission to do what you do also can get in a lot of trouble.

00;11;45;17 - 00;11;46;28
I learned that the hard way.

00;11;49;26 - 00;12;18;05
Jen:
Here's our challenge for this week will be giving out prizes for individual participation and team participation. So be sure to submit to the next two challenges to increase your chances of winning. The Episode five Challenge is now live on our website at WW Cryptologic Foundation dot org forward slash podcast. If you haven't tried to break a password before, this challenge will show you how easy or hard it can be.

00;12;18;25 - 00;12;35;28
Special thanks to Austen King for setting us up with this challenge. Good luck, everyone. And if you get the flag, you really are among the elite. I'll have you sign up to our mailing list on our website. You'll get notifications of when the leaderboard is updated and when new challenges drop.

00;12;39;11 - 00;12;48;28
Jen:
Okay, so like you said, you both work for NSA Center for Cybersecurity Standards. So what is that exactly? Can you kind of get into what you guys do?

00;12;49;14 - 00;13;20;00
Jessica:
So what CSI's mission is, is coordinating NSA's engagement in standards development organizations. Generally speaking, NSA and everyone uses standards all the time. Standards really underpin how computer systems talk to each other, how we protect our communications, how our cell phones work, and how your cell phone communicates to the tower, communicates the core network, communicates to someone else's cell phone, and how we protect our cloud computing systems.

00;13;20;09 - 00;13;57;07
These are all systems that we rely on to secure classified information. So here at NSA, our mission really is focusing on making sure anything that's classified is well protected. And Mike, my role and our team, which is an ever growing team, is to go out to standards bodies. Some of them are like national US standards bodies, and some of them most of them are international standards bodies where we're working the whole world to say, how are we going to ensure that this communication is secure or interoperable, or that we can set requirements to it so we can buy stuff that does the things we need it to do?

00;13;57;25 - 00;14;18;19
Jen:
You know, I'm from a education space, and maybe students are also more familiar with this. Like, standards are really important to making sure that all the students in the classroom and all their

classmates are, you know, they're taught the basics that they're needed at that level that they're at. So when they get to the next level, they have all the information that they need before moving on.

00;14;18;19 - 00;14;27;17
Right. Why do standards matter to cyber? You know, what are they? Are they like those sort of education, like standard IDs or are they something different?

00;14;28;08 - 00;14;49;07
Jessica:
They're a little bit different. So there's a certain amount of overlap there. What you describe, there's a certain amount of standards that are this is the most basic level of things you have to do. So we can say to computers, can talk to each other as an equal and and those who built those standards might add on additional things that go beyond the standard.

00;14;49;07 - 00;15;13;22
They might do something cool that differentiates them in the market, which is why you want to buy this cell phone and not the cell phone. Right. But all cell phones, what you can use, all cell phone call, any other cell phone that might meet that basic standard like you described. But what standards do in cyber security more is kind of set those requirements for what do you need to do in order to interoperate between two systems or what do you need to do?

00;15;13;22 - 00;15;33;25
And or I would say two systems meet the same level of security. And a lot of times these two things are not super different. But I think at the most basic level, nothing we do with our computers, it having this zoom call or or being able to use our cell phones or being able to log in and buy something off at Amazon, none of that works without these standards being written.

00;15;34;18 - 00;15;58;06
Jen:
So part of your work, I know, is to like upgrade these standards that depend on potentially vulnerable algorithms and I assume that's where the math background Mike comes in handy. So what makes these algorithms vulnerable? That's kind of what I was thinking when I heard about this like that. Does it make sense? Like why weren't they made secure to begin with?

00;15;58;06 - 00;16;02;24
So how are you working to upgrade these standards?

00;16;03;05 - 00;16;12;26
Mike:
That's a really reasonable question. Maybe I'll lay the groundwork by saying what's changed. These write these algorithms were secure and I would even say are secure now. Let's get that out there. They are secure today.

00;16;16;22 - 00;16;16;28
Okay. But there's a new technology on the horizon, and I would say even is here in very limited small prototypes. Okay. It's the idea of a quantum computer. So.

00;16;35;02 - 00;17;04;22

The computers we use, including the laptop that we're all going to talk to you, they're all built on the idea of bits, things that can be either zero or one. Okay, yes or no, zero or one two choices. So quantum computers really expands the range of the kind of data that can be worked on. So they allow for, I'll call it a probabilistic calculation, but it's basically a bit.

00;17;04;22 - 00;17;29;17
And the quantum computer doesn't have to be zero or one. It can kind of be like probabilistically, anything in between there. And that might sound kind of weird and science fiction maybe, but it turns out it makes that computer very good at doing certain problems. But today's computers are not good, that it does turn out that it's it's a revolution that's kind of on the horizon out there at some point.

00;17;30;04 - 00;17;55;07
Jessica:
And I think the reason we're concerned, the reason we say things like secure today that we need to do this transition at the same time is because there isn't this computer yet. There isn't a computer that we call cryptographically relevant quantum computer -- that doesn't exist yet. There people are experimenting with quantum computers, but the type of computer needed to do the kind of math that Mike was just describing, that's not here yet, but it could be coming.

00;17;55;20 - 00;18;32;12
And we at NSA, when we when we encrypt data, when we have a national security secret, we need to encrypt it. We need to be sure that no one can access it for 40 years. We have this longer time line than than most people do. The government has this longer time, and most people data where a foreign country who wanted to get at our national security secrets could be storing all our communications, could be putting it away somewhere and in the in a box and saying, well, when we get a quantum computer, then we will translate all this data that that NSA, that the US government still wants to be encrypted and we'll know their secrets.

00;18;32;12 - 00;18;45;07
So we are trying to transition to this new type of cryptography that isn't going to be able to be attacked by the coming post quantum computer today so we can protect our secrets for 40 years in my.

00;18;45;19 - 00;19;10;17
Jen:
Okay, so that makes a lot of sense because what I do know about quantum computers is they are capable of doing a lot of good math. Right. And to make an algorithm or encrypt something, you know, hide it from plain text, there's a lot of math involved in that. So that makes sense that, you know, a quantum computer might be able to do things way, way, way, way, way better than what we have now.

00;19;10;24 - 00;19;24;00
Okay. So that that really clarifies that. So that's the threat to current cryptography then, right? Is quantum computing in general, is it sheer power? And still there's unknowns about it, right?

00;19;24;19 - 00;19;46;14
Jessica:
Absolutely. And it's definitely one of those things that we want everyone to know that it's okay to still trust encryption algorithms. Right now. We do. We encrypt our stuff still using the same old cryptography that that that's used when you go to Amazon, which is when you log into your bank

account or go to check your grades online, there's communications are encrypted and they're safe For now, we just want to be sure that we're safe in the future, too.

00;19;47;00 - 00;20;01;26
Jen:
It's surprising to me that you mentioned that there are other countries that might not agree with some of these standards. And like I guess I'm curious, you know, how or what other governments think or how authoritarian governments would be threatening these standards in that way.

00;20;02;11 - 00;20;28;16
Jessica:
The way the Internet is set up is very decentralized. It's like no one's in charge of the Internet. There's no like, this is the body that decides what happens on the Internet. Wherever you go on the Internet, you're communicating simply with someone else's computer, right? So when you go to Twitter, you're communicating with the Twitter computers. And when you go to YouTube or the whole other set of people who run that show and have their own systems whole different set up.

00;20;28;27 - 00;20;59;16
A lot of authoritarian governments aren't super happy that Twitter, YouTube, any place you go secures that communication in whatever way they see fit, right? We have these standards and agreements, but like what exists on a particular set of servers is that companies information to control and a lot of countries who maybe want to monitor their citizens more carefully, they they don't like the idea that that information isn't under their control.

00;20;59;16 - 00;21;17;13
It's under the control of whatever computer you were talking to. Right. And so they definitely want access to that information and in a way that's kind of seamless in a way that they don't need to go to that company and say, hey, give me Jennifer this information from whatever site she was on. That's right. They just want to have it.

00;21;17;18 - 00;21;39;09
So a lot of what we're seeing is this push to create more centralized control of the Internet. And the problem for us is that they can't make that decision on their own, right. They can't just say, well, for China, this is how we're doing things, because we all kind of use the same equipment and we need to be able to see like people buy things from China all the time.

00;21;40;00 - 00;22;03;06
Your computer might go to Alibaba and buy stuff. You're free to do that. But yeah, they we can't have it be just like separate rules for them and for us. So they try to bake these ideas into standards where the standards are just written so that they can do this kind of monitoring, which is not good for the US or its citizens or definitely national security systems.

00;22;03;16 - 00;22;21;00
The standards community has actually done a really good job so far in pushing back on this kind of work. There are a lot of people who are really dedicated to a free and open internet, and this isn't like I don't want to come off as something that only NSA is trying to do. Like the standards community actually handled that problem without our intervention.

00;22;21;00 - 00;22;31;16
And it was great because they noticed what was happening. They said, Oh, but we don't want to use AI standards to spy on people. We want to comply. And we said, yes, that's what we want to.

00;22;36;11 - 00;22;52;26
Jen:
So how did you get involved with doing pen testing? Do you do it for a company? Do you do it through an organization? Like how did you find out about this sort of work to get this sort of experience, you know, on the job in college? A lot of people are looking, you know, in college for internships and things.

00;22;52;26 - 00;22;56;18
So it I think it would help others to know, like how to find these opportunities.

00;22;57;19 - 00;23;18;26
Austen:
Yeah. So I have a couple friends who are working for us, or it's called a grant funded organization. So the course the university has this building called Mat Labs and we have a bunch of organizations in it that use grants to fund certain projects. Some of these are like Iot hacking. So like device things hacking. Some of them do malware research.

00;23;19;16 - 00;23;33;26
And my instance, my the grant that I do is fantastic, like local counties and stuff. So we have this platform called handshake and I was told to supply and just take the interview and see what happened.

00;23;33;26 - 00;23;57;23
Jen:
So what recommendations do you have for those starting in cybersecurity other than, you know, don't be distrustful? You know, how does somebody go about like figuring out what type of field they want to be in? Like you've determined you want to move more towards red teaming. How do you like really just decide, is it something that you the work that you've done or is it a class that you've taken that's changed your mind?

00;23;57;23 - 00;24;20;11
Austen:
Many different ways, for sure. You could talk to people in the field here about their day, right? I mean, on LinkedIn, you can just add about anyone and it's filtered by the career path and they may or may not tell you what they do day to day. I mean, sometimes it's a little harsh about what they do with their given time because, you know, you can't just go around telling people, but you can also do competitions.

00;24;20;11 - 00;24;43;24
There are competitions in every aspect of cybersecurity at this point. And they and as well for every single like skill level. So you can basically just go through and find the competition that suits you best and like this might be what you want to do, but also to consider competitions aren't necessarily what actually happens in real life. So it's kind of like just trial and error.

00;24;44;05 - 00;25;02;12

That's kind of what I did. I started out in defensive. I enjoyed the competition, but I knew it wasn't for me. But I took those skills that I learned from like the defensive competition and I took them to the offensive side of security because at that point I knew what defenders were looking for and I knew how blue teams kind of thought because I was that blue team for years.

00;25;03;18 - 00;25;26;27
Jen:
What's the number one thing you think most people need to make sure that they do to secure their data? Because you've been in some systems may not be out of college yet, Austin, but you've seen more than most people have seen. So I think you have a unique perspective like what would be the top thing everyone right now could do to make their data more secure.

00;25;27;18 - 00;25;44;16
Austen:
For the individual user-- passwords. I mean, everyone says that, right? But like if you have a shared password across all your accounts, it's very dangerous because like, there are compromises every day. And if you give your password to a really sketchy website and it gets leaked, that email and password is going to end up in a database somewhere, I can almost guarantee it.

00;25;45;05 - 00;26;01;01
That's something we look for as we do searches on like different dumps for emails that we find of like people who work for a company. And we will try and use those passwords within their network as well. And occasionally they might catch something as well, which is scary.

00;26;01;20 - 00;26;09;07
Jen:
That is really scary. Good tip. So not just have a good password, change your password frequently, right?

00;26;09;07 - 00;26;10;04
Austen:
I'd say so, yeah.

00;26;17;15 - 00;26;29;00
Jen:
So you both come from different backgrounds of, you know, education and reflecting back on your job. So like, what skills would you need to be successful and keep moving forward?

00;26;29;18 - 00;26;53;09
Mike:
You know, the problem solving thing we talked about like I think it keeps going year after year is like the important thing. But I think flexibility, I mean, you can definitely see that neither of us maybe are kind of doing exactly the work that we went to school for. But at the same time, it's work that we find really interesting and enjoyable and useful and all that.

00;26;53;22 - 00;27;25;13
I think to some extent, you know what you go to college for. Maybe it'll be your career for your whole life, but it also may be just like teaching you to to think about things, you know, give you knowledge and

teach you to think and so forth. And I think that that that is the real value there. So I would say flexibility and definitely, you know, keep up with what's happening in the world, whether it's technology or politics or anything, but definitely be plugged into the world around you and understand how things are changing.

00;27;26;17 - 00;27;51;08
Jessica:
To your point about, you know, neither of us did exactly what are doing right now, what we went to school to do. But but a lot of that isn't even necessarily because we found other interesting things, because other interesting things happen to the world and we needed to pivot quick in order to help address that. And we're seeing that even our work right now, like we were very comfortable, certain sets like protocol standards, we've talked a lot about them because that's where we both started out.

00;27;51;08 - 00;28;21;16
So we're good at those. But there are new standards that are coming up that we are having to educate ourselves on really quickly. Emerging technology you mentioned and all that, that's going to be huge. And we need to educate ourselves in order to engage in those sense and how to make machine learning processes trustworthy so that we know for national school systems that the machine learning isn't being meddled with and being taught the wrong thing in order to make the wrong decision for us and we need to use it.

00;28;24;16 - 00;28;43;14
Jen:
That's our show. Thanks so much for being a part of our community. We can't wait to see how you do with this week's episode challenge. Go to the CyberChats podcast page on our website at www.cryptologicfoundation.org to find this week's challenge, submit a question and join our focus group to help improve the podcast.

00;28;44;15 - 00;28;56;29
You can watch more of this podcast on YouTube. Be sure to like and subscribe to hear more and check out the show notes for more details and links. This podcast is made possible by the Chilton Foundation.