Oral History Interview with

Dr. Chuck Easttom

March 8, 2024

Video Conference

Conducted by Yi Fong LOH

Charles Babbage Institute

Abstract: This oral history interview is sponsored by and a part of NSF 2202484 “Mining a Useable Past: Perspectives, Paradoxes, and Possibilities with Security and Privacy,” at the Charles Babbage Institute. The interview begins with Chuck Easttom recounting how he got interested in computers. His interest developed from reading magazines and gradually taking up part-time jobs repairing PCs. He describes his developing interest in cybersecurity alongside the wide range of experiences that inform his work. He describes how his consulting business at Chuck Easttom Consulting grew. Described how the Certification industry was like. His first court work from 2004 as patent cases, before a private investigator's license related to digital forensic work in Dallas, Texas. Describes experiences publishing textbooks. Discusses the education of next generation of cybersecurity professionals. He related his experiences mentoring in a firm as compared to the university, and the implications of newest quantum computing technology for security at Vanderbilt University. The interview ends with final reflections on generative AI and the meaning of being an engineer in contrast with simply using the word when being a programmer.

Keywords: TSR-80 Radioshack, Omni Magazine, Southeastern Oklahoma University, Vanderbilt University, cybersecurity, network, AI, PC repair, standards, certification, patent case, digital forensics, digital forensics, software development, textbook publishing.

Loh: It is March 8th, 2024, and this interview for the Charles Institute National Science Foundation funded project, mining a usable past, perspectives, paradoxes and possibilities in security and privacy. I'm here this afternoon with Dr. Chuck Easttom. This is an oral history being conducted over Zoom. To start with just a few biographical questions, can you tell me when and where you were born?

Easttom: That's odd, I was born in Bangkok, Thailand in 1968.

Loh: Oh, would you like to just tell me a little bit more?

Easttom: Well, I know I don't look Thai, I do get that a lot. Back in the sixties, the US military had a small presence in Thailand, and my father was career military. He was stationed there, and thus I was born there. I have returned a couple of times since then, and because I was born there, my passport, although it's US, actually says born in Thailand, and the Thai customs people every time I've been, looks at it very strange and looks at me thinking, you really don't look Thai.

Loh: Yeah, that's fascinating. Could you describe yourself as a student in your pre-college days? What were your interests like?

Easttom: I had a difficult time settling on one interest because so many things interested me, most of the natural sciences, chemistry and physics, mathematics, computers of course. I suppose I followed through on that, which is why I have well, far more college degrees than most people normally do simply because I continue learning, and in fact I'm going to school now to work on more degrees.

Loh: Could you describe your time as an undergraduate at Southeastern Oklahoma State University?

Easttom: Well, I changed majors a lot because I was exploring a lot of different things, everything was interesting to me. I really enjoyed the campus. It's a smaller campus, but a little more close interaction with faculty. A beautiful campus, replete with magnolia trees. There's a really good and enjoyable time for me.

Loh: How did you really think you pivoted towards computers, or in your formal education, or in that long prelude?

Easttom: I had been working unprofessionally just as an amateur with computers since I was a teenager using really old computing systems you couldn't find anymore. This was in the days of things like the TRS-80, very old computing systems. Radio Shack made a computer you could use, and by the time I got to university, I

continued to use computers even in my other work. For example, I wrote some programs for the chemistry department when I was working on chemistry classes. Eventually, I ended up doing side projects for money writing programs, things of that nature.

How I eventually got professionally writing code is I was in a Usenet newsgroup in the very early nineties, and I was in a group devoted to programming and this gentleman kept asking me questions, and I kept answering them in detail. He finally told me that he was a manager for Boeing Aerospace, and would I be interested in a contract programming job? His way of screening out people was to ask them questions online, and from there the rest of my career was all in computer science.

Loh: Where were you when you first used TRS-80 RadioShack as a teenager, you mentioned?

Easttom: Well, I was living in eastern Oklahoma at the time. This was in the eighties, and it was basically a small computing device. You had to plug it into an old television set for a monitor, and it used magnetic tapes to store data.

Loh: Were you introduced to it by the people around you, or as a teenager how were you drawn to the device?

Easttom: I saw an advertisement for these again and again in the back of a magazine that no longer exists. It was called Omni Magazine, and what Omni specialized in was really cutting-edge scientific articles, but written for the lay person, so you didn't have to be a scientist, and they would only focus on the really exciting stuff, altered states of consciousness, things like that. I would routinely go to the library and read Omni Magazine, and I had continually seen these advertisements, and was eventually able to get together enough money to get one.

Loh: You mentioned your informal interest at a site with computers proceeded your formal education?

Easttom: Correct.

Loh: Could you describe when the first jobs that you were getting pivoted more towards when you started working with computers?

Easttom: Well, at the same time I was at university, early on I had gotten a part-time job at a computer store, basically building and repairing custom PCs. This is in the days of the IBM XT, when a standard

computer would have maybe 640 kilobytes of RAM and might or might not have a hard drive.

If it had one, it would be 10 or 20 megabytes of hard drive, and I would build and repair these, and then I began doing small programming jobs for example, and these were all DOS based programs, no graphical user interface. But a program I wrote to manage a quarter horse ranch, where quarter horse-racing horses they raised I would manage all their material on a computer. I wrote software for that, and I just kept writing these smaller applications until I eventually got a contract with Boeing Aerospace, working on the NATO, a work software.

Loh: When was the first job you took, if you remember?

Easttom: My first paying computer job would've been about 1992.

Loh: This would be right after your undergraduate degree, which ended in 1991?

Easttom: No, I was actually still going to college. Back in those days there were a lot of people in the computer industry that had no degree at all, or they had no computer science degree. I was actually working and going to school part-time, and that went on for quite a few years. I ended up not completing the undergraduate degree until 1998, because I was working at the same time and going to school part-time.

Loh: You spent a great deal of time developing websites with HTML, with JavaScript, which was introduced in the late 1995, but how did you see the tradeoffs then between the goals of interoperability and moving quickly, versus a score at security design?

Easttom: Well, unfortunately in those days, most people weren't thinking about security, which is one reason you had so many early hacks that could never occur today simply because they were so easy to do. The security flaws being introduced in systems in those early days were simply obvious terrible flaws, 'cause no one was even talking about security. Now by the late nineties, at least some people were starting to think about security, and it was probably 98 or 99 that I started getting very seriously interested in as a side note.

Unfortunately, the biggest problem we have in cybersecurity, is we often wait until a problem has become very large before we address it, case and point being ransomware. To all anyone can talk about today, and the first major ransomware that most people know about,

was CryptoLocker in 2013, but the actual first ransomware in the real world that was ever discovered was in 1989, but we as a computer science community didn't get serious about countermeasures, until huge amounts of damage were done.

Loh: I'm just going to ask a bit more specific questions on the same organizations in the nineties before we move on. Were there different degrees and types of regulations within different industries such as banking, finance, automobiles that paid up into the needed specification for software system designs in the second half of the 1990s when you engaged in software engineering, for various corporations or clients?

Easttom: Sure. By that time, you were starting to see the National Institute of Standards and Technology had produced standards, IEEE had produced standards. There were clear software engineering standards. The problem we had then, and we even still have today, is so many people in the software business are not following real software engineering. They don't do the design, the planning, the standards, the testing, they just write a lot of code and hope it works, and that's unfortunate.

Loh: How did your work experiences at this point relate to your interest as you transition towards teaching networking?

Easttom: Well, I still do work practically. I do a combination of practical consulting work and I do teaching, but eventually I realized that too narrow a focus made it impossible to really be effective. In other words, if you just looked at programming without also considering hardware networking and things of that nature, you would find yourself very, very limited, and there'd be things you didn't know simply because you'd over limited yourself. To this day that's a philosophy I follow.

I think too often people have such a narrow focus that they're not aware of answers to their problems that are already found in other related areas. For example, you might have someone who only focuses on web programming, and knows virtually nothing about networking and hardware, and there may be solutions they could use, but they're not aware of simply because it's not in their narrow area.

Loh: This connects a bit to the point of education. You mentioned you spend a fair bit of time in postgraduate studies. Could it tell us how you ended up pursuing your first master's degree?

Easttom: Well, I had been working as a software developer for some time, and I know there are a lot of soft self-taught programmers out there, but I became concerned that there were things I might have missed by not doing formal computer science degrees. I decided to go back to school, and work on a master's degree in applied computer science. Now I enjoyed it so much, I eventually went back to school and by now, I currently have three master's degrees, and three doctoral degrees. I'm just about this semester, in fact, going to finish up a fourth master's degree, and I'm in the process of working on a fifth one.

Loh: If you remember, when did you start the master's in Applied Computer Science?

Easttom: That would've been in the very early two thousands. Very early.

Loh: In 1998, you became the director of academic computing for Southeastern Oklahoma State University, where you managed all the technical support for the campus, as well as overseeing network administration, network security, and web development. Could you describe a bit of your job then?

Easttom: Well, the university had a combination of mainframe computers that were used by finance and registration, and then most professors had a small personal computer. There were personal computer labs for students, there were also a large MAC lab for the graphics design and journalism students, and my job essentially was to oversee the maintenance and support of all of those systems.

Loh: I guess in the 1990s, I don't imagine many people who could manage all parts of the computer network. How did your role as the director of academic computing differ from the people in the larger community then?

Easttom: Well, it's the same thing that has gone on throughout my career. I really paid attention to a wide range of topics which paid off in that job, because there were so many different aspects of computers to understand. There was networking, there was web pages, there was Macintosh, there were Windows computers, Windows 3.1, But it was important to have a wide range of knowledge, and throughout my career then and now, I see so many people are too narrowly focused, at least in my opinion.

Loh: In 2005, you started Chuck Easttom Consulting. Could you tell us how that got started?

Easttom: Well, that was a weird one because frankly, I was working before that full-time as information systems director for an insurance company, but by that time I had published my first few books, and I would constantly get calls from people who wanted me to do side projects.

I would end up working nights and weekends on these side projects, and eventually they became so important, and frankly made enough money that I no longer needed the regular day job and wanted to go full-time working for myself. What was interesting is by the time I finally gave my resignation, everyone at the company I had been working at told me, they had expected this any day now, because they all knew how much consulting I was doing on the side, so it grew organically.

Loh: How did the scope of work at the consulting company change gradually? Were you particularly targeting particular industry verticals such as banking, healthcare, automated or others?

Easttom: Well, that's a strange thing. I have never actually targeted anyone. I don't do any advertisement, I don't go out pursuing particular clients. It's simply the fact that I do a lot of speaking engagements. I've written a lot of books, and over time companies find me, and that's been in a lot of different industries. There have been financial, medical, defense departments, just a wide range of industries and I really like it that way, because I like keeping a diverse workflow.

Loh: How would you situate Chuck Easttom Consulting then alongside other companies? Did you differentiate your firm, or was it really a lot on the word of mouth rather than marketing per se?

Easttom: Well, there there's absolutely no marketing, so it has to be word of mouth, and it is just me. I don't have employees or anything, but I do keep very busy, and I have for many years now, I always have a large number of projects to do, and it's just happened over word of mouth.

Loh: Were you also a member of like trade or technical associations, or a member of ACM, the IEEE Computer Society and such professional organizations? Was it helpful to stay current and contribute to your work at the same time?

Easttom: Well, I've been involved in ACM and IEEE for a while. I worked in IEEE standards groups and things of that nature, but I'm not sure that that's really contributed to work projects. That's more research that I do, related to IEEE standards. I publish research at

conferences, things like that, I don't know that having spilled over into actually getting more work.

Loh: Industry certifications did become prominent in the two thousands, alongside when you mentioned that a lot of your books were coming out, could you tell us how industry certifications got started?

Easttom: Well, probably one of the very first certifications was Comp T is A plus PC certification. That's been around for over 30 years now, and the goal of that was to ensure that people who were working on fixing personal computers were certified. Now, over time, other people began to generate certifications. Microsoft got in very early in the mid-nineties creating certifications, so that if you needed someone to run a Windows NT server, you knew they knew Windows NT because they were certified. Now certifications have become a little bit controversial because some people either over or underestimate what a certification means.

In my opinion, a certification is a good thing if you understand what it means. It means that you have achieved a certain skill level on a certain set of objectives. It does not mean that you're the master of everything in that area. For example, if you have the CISSP, that means you have achieved a certain level with those specific objectives and that's a good thing, but it doesn't mean that you know everything and you're an expert in all parts of security.

Loh: At the same time, you were also a Texas State licensed private investigator in investigations and security, when did you begin acting for litigation support as it related to security?

Easttom: Well, my very first court work began in 2004 and it was a patent case, and that's different than the private investigator license. Where I live in Texas, is one of many states that requires someone doing digital forensics to either be retired law enforcement, current law enforcement, or have a private investigator's license, and so I've had a PI license over 10 years now related to my digital forensics work.

Loh
Easttom

Loh: What was Texas like as a hub for security work?

Easttom: Well, I specifically live in a suburb of Dallas, and we have a lot of major security companies here, like McAfee and people like that, so there is a lot of interest in cybersecurity in this area, and there always has been. As with any other organization though, we have a wide range of different companies. Some do a very good job of

security, some not quite as good, so I suspect it's pretty similar to most large cities.

Loh: How did it feel different when consulting for government versus industry?

Easttom: Well, the big thing is that government tends to move slower. Getting approval for projects takes longer. There's a lot of paperwork, a lot of steps involved. Depending on which part of the government you're working with though, it can be quite rewarding because you'll find some very, very dedicated people. For example, in the defense department, they have a very pressing need for whatever skill they're trying to learn or whatever consulting they need, and their interest and focus is pretty good.

Loh: While you were working as a consultant, were you also like adjunct professor at Collins College, for instance, in 2003?

Easttom: Yeah, for many years now I've been teaching and consulting. Nowadays I'm an adjunct for Vanderbilt in Georgetown and have been for a few years. I love teaching and frankly, that's something I would never give up. If I tomorrow won the lottery and had hundreds of millions of dollars, I still would keep teaching. I just love doing it.

Loh: Alongside your various jobs, you began publishing many textbooks, but how did the teaching of cybersecurity change over the years?

Easttom: Well, to begin with, it's gotten a lot more diverse. There are a wide range of cybersecurity courses taught now, instead of just general cybersecurity. For example, there's secure software engineering, there's penetration testing, a large range of things. There are also more resources now. For example, if you're teaching a class, there are companies that will have a complete online lab you can use with your students, to make it easier for them to actually do the things you're teaching. I think it's become a lot better, a lot easier to do.

Loh: There has often been a shortage of cybersecurity professionals in the past three decades, did you see certifications as helping to address this challenge? What about the NASA Centers for Excellence programs at universities and community colleges for certifications for research, and a separate one for education?

Easttom: Well, those programs at least help provide a baseline to make sure that the university is at least meeting that baseline, but any certification program you have to understand, should be looked at as the foundation, the starting point, not the end. In other words, if

you have a program, and their cybersecurity teaching program has been certified, like through the certification you talked about, that doesn't mean that it's necessarily the greatest program ever, it simply means that it's got that baseline requirements. That's a good thing, but that's a starting point not an ending point. I do think overall it is improving cybersecurity education, but I still think we have a lot of improvement still to do.

Loh: Could you walk me through the process of writing your first book, from getting hooked book publisher to its topic?

Easttom: Certainly. There was a very, very small publisher that no longer even exists called Wordware Publishing, and they happened to actually be in the Dallas area, and I ended up encountering them accidentally, and they were looking for someone to write a book on JavaScript, and frankly, the amount you would earn off writing the book was very small, so they were having trouble getting well-known authors to do it, but I wanted to write, so I agreed to do it.

I have to confess that the amount of money I made off of royalties for that first book [only applies to the first book], I probably would've made more money delivering pizzas on the side than I did off the book, but the book went reasonably well from their perspective. I ended up doing four or five more books with them, and after I had written four or five books, then more serious publishers would take me seriously.
My first major textbook was with Pearson, which is a major textbook company, and I've loved working with them, and I still work with them today. In fact, I'm working on a project with them right now, but it started off as with most things, very low money, working for a very small outlet, and basically learning the publishing business, learning the writing business, getting my name out there to the point that more serious publishers would pay attention to me.

Loh: Was this writing of the textbooks linked to your later creation of the OS forensics certification tests and courses? Could you tell us a little about that?

Easttom: Well, I don't know if it was related to the textbooks, but OS Forensics is a really great tool, and I've been using it for a long time, and at first, they did not have any certification like many of their competitors do. I simply reached out to them, I said, look, you have a great tool here, but there's no way for someone to get certified in it, and they arranged for me to develop their initial certification.

Now, I don't do it anymore, they've taken it inside, and their inside experts develop the new versions of it, but it was a really, really great experience, because I had to work in depth with the tool itself to learn it well enough, to create an entire certification course for it.

Loh: Was this similar to how you later also assisted Comp TIA in the creation of the security plus, Linux Plus and server plus certification tests, and on the job task analysis team for CEH V8?

Easttom: Well, with Comp TIA and the Computer Technology Industry Association, they will put out calls periodically for experts in fields to work on a revision or a new certification. I like the process they use. They bring in quite a few people, usually a hundred or more, and they divide them into groups, working various aspects of the certification test. They get input from a lot of different people, which is very helpful.

Now, EC council, I have worked directly with them for a long time. In fact, I worked directly with the Vice President for North American Affairs quite a lot, and so he knew who I was, and when they were doing the CEH version 8, he asked me if I would be interested in working on part of that team. Now it's not just me working on it, there's an entire team of people, but that's how that came about.

Loh: You've been consulting and lecturing for a long time, do you see your orientation as a practice-oriented cybersecurity professional as different from the more mathematically inclined like security professionals, if so, how has this relationship changed over time?

Easttom: Well, you mentioned mathematically inclined. I wish there was more mathematical inclination in both cybersecurity and computer science in general. I find that a lot of people want to jump into programming or into cybersecurity without having any understanding of the mathematics that could be used, and there's a lot of really great math that's not being used because people don't know how.

For example, my third doctorate, my dissertation was about how to use graph theory to model network intrusions, but you can't do that unless you know the mathematics of graph theory. I would say unfortunately, there's not enough interest in mathematics in the cybersecurity or software engineering fields, and I wish there were more.

Loh: How is your philosophy towards educating the next generation of cybersecurity professionals? Do you take graduate students also?

Easttom: Well, right now I only do two types of teaching. Either I teach graduate students, which is what I do for Vanderbilt in Georgetown, or I do corporate training for professionals. In both cases, I have a philosophy that first and foremost says, I need to bring them as much information as humanly possible. In other words, I need to know much more than the class requires, so that I can answer whatever questions I have. I need to make sure my knowledge is up to the date, up to the minute, and that I'm doing everything possible to educate them.

I view teaching as an honor to be able to teach, and I feel as if I always have to improve it. I have never taught a class that I did not, after the class was over, think about ways I could have done a better job, and so I'm always revising my curriculum, updating it. I'm always looking into new ways to teach both information to teach, and the actual curriculum that I teach because I'm always concerned, is it good enough?

Loh: You have extensive experience as well testifying as a cybersecurity professional, could you run us through that from how you got into your first case?

Easttom: Well, I mentioned previously that my very first case was actually a patent case, and I still do a lot of those, but because I also have experience in cybersecurity, I get called for those kinds of cases, and normally it breaks down to some stages. The first stage is analyzing all the evidence. In fact, Monday I'm going to collect forensic evidence on a cybersecurity case. I collect the evidence and analyze it, then you write a report.

Now, something I tell students that people don't always get is, the United States court system is adversarial, so when you write your report, you need to understand that the other side is going to have an attorney and maybe their own expert. It's going to basically try to pick holes, find flaws in your work, and I find that to be a wonderful challenge because it means I have to really do excellent work, because someone else is going to be out there trying to find flaws with it.

Now, ultimately, what you've gone past that process, the next step is going to be at some point testifying, whether it's testifying in a deposition or at trial. A lot of people find that a stressful experience, I haven't, but it's all about making sure you fully know everything in your report, know the basis for your opinions, and simply tell the truth.

Loh: With biological forensics, there are challenges with technical evidence, and analysis in communicating ways in which juries or judges can understand with cybersecurity and digital forensic testimonies. Can you describe the process in perhaps the art of communicating highly technical ways, information, in ways that the juries and judges can grasp?

Easttom: Well, I think you just asked the exact best question you could have asked about that, because it does come down to communication. You've got to be able to take a technical topic, explain it to a judge and a jury in a way they can understand it, without talking down to them. That's why a lot of attorneys like to hire professors for that work, because they have experience teaching. You have to balance between making sure you give them enough detail that you're fully explaining, and making sure you don't talk down to them, or over talk go into technical detail.

I'm a huge fan of a quote from Albert Einstein. He said, if you cannot explain it simply enough, you don't understand it well enough. You can take any topic. You could take quantum physics and you could explain it to a child, just leave out the math, and I think a mistake I see people make, they get on the stand as expert witnesses, and they try to impress you with how much they know, and they end up alienating the judge and jury because they don't understand what they're saying.

Loh: How does mentoring in a cybersecurity firm differ from that in a university? Could you name a specific relationship and contrast those experiences?

Easttom: Well, I would say in the corporate world, the mentoring is probably going to be more focused. We have specific skills we'd like this person to develop, we have a timeline we're looking at, whereas in a university setting, the person doesn't necessarily have a very specific goal, and what you're trying to do is broaden their horizons.

Also, sometimes in the university, you're trying to help them with research skills, things of that nature, which wouldn't be a part of the corporate world, so there's a bit different focus in the corporate and in the university world, and in the university world, it's usually a little broader, whereas the corporate world will be more narrowly focused.

Loh: Your work has also shifted towards considering the implications of newer technologies such as quantum computing for security, would you like to elaborate on that?

Easttom: Well, I did my first dissertation on quantum computing and its impact on security, and now one of the classes I teach for Vanderbilt is a graduate course in quantum computing. Anytime there's new technology, there are going to be security issues. Now with quantum computing, the security issues are obvious, because quantum computing can break current widely used public key encryption algorithms like RSA and elliptic curve.

There's an obvious interest in understanding how to mitigate that threat, but what I see in the cybersecurity world in general with new technology, is unfortunately we will often wait till the new technology is out there, and wait till it's been breached, or it's been misused and then start thinking about security. When I think of any new technology, chatGPT, augmented reality, any of those things, the first thing that enters my mind is how are we securing that?

Unfortunately, I don't think that always enters the mind of the vendors that are creating these products. We frequently get products out already in public and then later find security issues. A classic example would be the doorbell cameras. When those were first released, they were being breached constantly. The news was replete with stories of people taking over your doorbell camera, and then later we came back and made them more secure. I think the issue is that when new technology comes out, it's important for the vendors of those new technologies to be thinking about security from the very first day before you even release the product.

Loh: Looking back at your more than three decades in computer security and systems engineering, are there lessons evident from the past that have not been learned or not fully learned?

Easttom: Oh, absolutely. One of which I just said, we need to have security from day one. If you're writing a website, if you're developing an app for the iPhone or Android, from the point when you first start doing planning and design, you need to be thinking about security, because if you try to add security later to an existing product, it's going to be a problem.

One of the things I do with students is, every class when it's related to software engineering, I start off with a classic case study of software that went really, really bad and caused lots of damage, so we have it, got that security from day one. We also, particularly in the software industry, are getting very lax, because if there's a problem with your software, you can always release a patch and automatically patch it, and that gets us to release software that

maybe shouldn't have been released yet, because we think it's okay, we'll just put out a patch.

I think we've gotten to rely on that and we're not doing good engineering. We're not really doing really good planning, designing, testing before release, and that's been the case for as long as I can recall, and I don't see it getting any better today. We've had a few issues related in one way or another to security and to software engineering quality, that we just don't seem to learn. We keep making the same mistakes again and again and again.

Loh: What is referred to as generative AI, is being deployed by organizations to find vulnerabilities, pre software system release by blackhead malicious hackers once systems are released, and by white hats trying to protect systems and detect perpetrators, how do you view this dynamic in the present, and what is your expectation for what might develop in the years and that case to come?

Easttom: Well, I would first say that any tool that's out there, malicious actors are going to use. The fact that we're seeing malicious actors use generative AI is not a surprise to me. I fully expected that, of course, they were going to. I'm glad to see that some of the security professionals are also embracing it to do things, like you said, look for vulnerabilities, things of that nature. Now we're also seeing generative AI that were specifically made for misuse.

For example, FraudGPT is a generative AI that's available on the dark web. Its whole goal is to help make fraud and phishing emails and things of that nature, so we're seeing things like that happening. Now, the answer isn't to avoid new technology because you can't, once it's out, it's out. The answer is to be aware that any new technology we release is going to be misused, and to begin looking for ways to mitigate that as early as possible.

Loh: Are there topics I've not covered or themes I've not addressed with my questions that you'd like to discuss?

Easttom: Well, I would go a little further with the generative AI. I get asked about this a lot lately, and one particular issue are the deep fake videos. A lot of the people I consult with, particularly in various government groups are very interested in that, because it used to be said, there was an old saying, a picture is worth a thousand words. It meant that if I have a photograph of something, that was the best evidence you could possibly have, and a video, oh, wonderful. Well, now you have to ask yourself, is the video or the picture even real?

We're seeing a lot of fake videos and fake pictures that are changing our view of evidence. Just because I have a picture of something does not mean that that's reliable evidence. We're seeing deep fake videos being used even in things like child pornography, which is very disturbing.

Unfortunately, we're seeing a lag in the legislative bodies coming up with laws. There are some laws out there that work to try to mitigate this, but not enough. I would say that, as we get new technology, it's also important for there to be regulations and laws governing the use of that technology, so that we try to at least limit the misuse of it. I think generative AI is gonna continue to be a major issue.

We're seeing more and more improvements in AI to the point that I would now say, if you're majoring in computer science, you absolutely should take at least one AI and machine learning class, even if you don't wanna specialize in that. If you want to be a network administrator or a software developer, it's becoming so prevalent that you simply can't work in computer science without some basic knowledge of AI.

Loh: Are there still more topics that I have not covered or themes I have not addressed with my questions, that you'd like to discuss before we conclude?

Easttom: There is one I am concerned with that I talk about a lot since you're giving me the opportunity, I'm gonna talk about it now, the word engineering. In the computer world, everyone likes to call themselves an engineer. You don't have programmers; they say they're software engineers. No database admins, they're database engineers. Well, engineering has a meaning, and it doesn't mean just working with technology.

For you to be an actual engineer of any type, whether it's an aerospace engineer or software engineer, means first of all, you're very familiar with relevant standards, and secondly, you are doing things like design, planning, testing. Think about an aerospace engineer. He or she may never go out to the factory floor and actually bolt something onto an airplane. What he or she did was create detailed plans, designs, test cases, modeling, things like that. In the IT world, we're not doing that.

We're calling ourselves engineers, but we're not doing engineering, and that's most true in both software and cybersecurity. Cybersecurity, if you're going to be a cybersecurity engineer, that

means you've got standards, you've got planning, you've got modeling, you've got design, you have metrics to understand your risk profile, things of that nature. If you don't do that, then you're not an engineer, it's that simple.

Particularly with programming, I see anyone who writes code calls themselves a software engineer. Well, simply writing code does not make you a software engineer at all, unless you took those engineering steps, and probably the worst abused title is systems engineer. That title gets used for network admins, for tech support people.

Systems engineering is a very defined discipline, founded and managed by the International Council of Systems Engineers, of which I'm a member, and there are specific requirements to be one. I would like to see us not stop using the word engineer but start actually doing engineering. Throughout computer science and cybersecurity, I would like to see more actual engineering, and that's my last extra item I wanted to make a point of.

Loh: Thank you so much for your time and your thoughts. That's all, I could end the recording.

Easttom: Okay.