EPISODE 798

[INTRODUCTION]

[0:00:00.3] JM: Steve Herrod was the CTO at VMware and now works as a managing director at General Catalyst, where he focuses on investments relating to security. General Catalyst is a venture capital firm. Large enterprises are difficult to secure and that's why investing in security companies is pretty interesting.

An enterprise has sprawling infrastructure with both on-prem and cloud infrastructure. There's identity management systems, vulnerability scanning, secure network infrastructure, policy management tools. There are so many areas where enterprises spent billions of dollars on security software.

Threats often make their way into an enterprise by way of social engineering. This can result in phishing attacks, corporate espionage and ransomware. Protecting against social engineering is very difficult as there are so many channels to communicate through; Facebook Messenger, LinkedIn, e-mail, ad networks that are just appearing on the internet, all of these things can be used to perform social engineering attacks.

Enterprise security software is a very different business from other types of software companies. Unlike developer tools or cloud infrastructure, security software is usually not self-serve. Security solutions usually require a longer sales and integration process with a customer.

Steve Herrod joins the show to talk about the enterprise security world and the go-to-market strategy for successful security companies, as well as his perspective on what makes for a viable venture capital investment. Steve was a previous guest on the show talking about his early experiences at VMware and his perspectives on the cloud and the edge. Today's show is a great adjunct to our last episode.

Before we get started, we have a few events coming up. We have a hackathon for my new company FindCollabs, which is April 6th. We have a meet up with Haseeb Qureshi on April 3rd. The hackathon is a virtue hackathon and an in-person hackathon. You can find out more by going to softwareengineeringdaily.com/hackathon, or findcollabs.com/hackathon. That's an event where you can share your open source projects, you can share your art projects, your music projects and find collaborators using FindCollabs.

There's a first-place prize of $4,000. Second-place prize of $1,000 and plenty of other prizes. It'll be a lot of fun. The in-person event on April 6th is at App Academy. We'll have some food, we'll hang out, we'll hack on some projects together and I hope to see you there. Our meetup, which is on April 3rd will feature Haseeb Qureshi, who is a frequently requested guest on Software Engineering Daily. He's a good friend of mine. He's a savvy investor, cryptocurrency, entrepreneur and also former poker player who I met back in the poker days. We have some shared history and it's going to be a lot of fun on April 3rd.

You can find out about that event by going to softwareengineeringdaily.com/meetup. I recommend signing up for both of these events quickly, because space will probably run out. I hope to see you there. Let's get on with today's episode.

[SPONSOR MESSAGE]

[0:03:41.1] JM: Deploying to the cloud should be simple. You shouldn't feel locked in and your cloud provider should offer you customer support 24/7, because you might be up in the middle of the night trying to figure out why your application is having errors and your cloud providers support team should be there to help you.

Linode is a simple, efficient cloud provider with excellent customer support. Linode has been offering hosting for 16 years and the roots of the company are in its name. Linode gives you Linux nodes at an affordable price, with security, high availability and customer service.

At linode.com/sedaily you can get started with 2 gigabytes of RAM and 50 gigabytes of SSD for only $10. There are also plans for cheaper and for more money. Linode makes it easy to deploy and scale your application with high uptime and simplicity. Features like backups and node balancers give you additional tooling when you need it.

Go linode.com/sedaily to support Software Engineering Daily and get your application deployed to Linode. That's L-I-N-O-D-E-.com/sedaily. Thank you Linode for being a sponsor of Software Engineering Daily.

[INTERVIEW]

[0:05:09.5] JM: Steve Herrod, you are an investor at General Catalyst. You're a former CTO at VMware. Welcome back to Software Engineering Daily.

[0:05:16.2] SH: Thanks, Jeff. Good to be here again.

[0:05:18.3] JM: You've been an investor since 2013. How has the security market changed in the last six years?

[0:05:25.1] SH: Yeah, that was the area that I thought would be most interesting to start my investment career in after being at VMware and dealing with enterprise companies for a while. The good news is it continues to be a very good market and I think as measured by the amount of spending going on at customers. Security obviously continues to be a huge problem for all of them. It's one of the few areas where end-customers are increasing their spending.

The good or the bad news is that the types of attacks are getting even more sophisticated and by stronger organizations, so the need for solutions to improve technology-wise has been growing. That makes for a great investor space; lots of spending and lots of disruption to be made.

[0:06:04.2] JM: When you were at VMware, what were the biggest security concerns that you saw?

[0:06:08.7] SH: It’s funny, at a top level the same type of threat continues to be the number one threat, which is tricking people into doing something. Whether that's phishing, or new forms of malware, or the latest form of how you get an employee to open that attachment, they're coming in different forms now, but that continues to be the number one way that companies get infected; someone will open something, ultimately granting their privileges to a bad third party and then that third party can pretend that they’re Jeff and a company and go off and do stuff under their name and get data and that sort of thing.

The same core problem has been there. It's just now we have new forms of channels for people to communicate over a Slack or something like that and far more sophisticated ways of personalizing a note that goes out to you to get you to do something.

[0:06:56.0] JM: Are you seeing Slack phishing attacks?

[0:06:57.9] SH: I think it's the beginning. I'm seeing the early signs of all of these other channels that we communicate over, whether it's something like, Slack, or text messaging, or even documents and collaborative documents is something we all spend time on now, whether it's a Google Doc or a 365 doc. People are able to collaborate in those and cause some malware to be distributed through those as well.

[0:07:16.9] JM: Yeah. I got a unsolicited LinkedIn message this morning from somebody sending me a PDF and talking about investment-related subjects, like here's the investment document. I'm like, “What?” I definitely did not click on the PDF, but –

[0:07:31.9] SH: PDFs are in particular I'm seeing a growing amount of malware being distributed through them. It's a whole programming language PDF. Previously for old-school listeners, I see a postscript was a full programming language, and so you could embed a lot of nasty stuff in those.

[0:07:45.7] JM: You were at RSA recently. What was the best anecdote about modern security that you heard there?

[0:07:52.0] SH: What I've noticed is that on every single RSA, there's some different theme. The theme comes in the form of both what types of attacks people are talking about on one side. Then there's definitely a thematic what is the hot new technology that we should be looking forward to. There's always optimism, like what is the one that will finally solve the security problem? Obviously, they never solved everything, but they moved the bar forward.

This year, I think the notion was really focused on I saw it as trust no one. All the ways people are doing phishing attacks are getting more sophisticated. Insider threats are very big. It's all this notion of whether it's machines or humans, it's getting even trickier to believe anyone, which is sad. I guess it falls into the fake news world as well. Who do you trust being one thing? Then as a result, the type of solutions being discussed a lot are what are called zero trust architectures.

The core of zero trust means basically that trust no one. It used to be that at least if you were within your firewall, or within your data center, you could believe the machines were going to be fine. Now it says, “Hey, don't even believe that. Let's authenticate every single server, even if it's inside our own data center walls.”

[0:09:02.5] JM: Yeah. It seems there's a lot of other advantages too, because if you have different – if you have different shades of contractors also coming through, then the notion that our default is we're not going to trust this individual becomes much more practical.

[0:09:17.6] SH: It does. Definitely you could argue we're in a more and more gig-oriented world with more and more alternate workforce workers. What I find interesting is that the line between an internal worker being negligent versus being actively bad, it doesn't matter, because if you get – if someone gets into your account and then becomes you, that's the same thing as if you were a bad actor doing things internally. I don't really see the solutions being particularly different to a contractor versus an internal employee in this zero-trust world.

[0:09:48.1] JM: Were there any other broad takeaways from the conference, any strange or subtle themes? Maybe things that don't seem they're big today, but maybe bellwethers of what you're going to see be the big zero-trust level theme of five years down the line?

[0:10:04.1] SH: Good question. That's really what my job is to try to do is to find the next big thing, not the one that everyone just invested in and is happy with. It's easy to be sarcastic about it or very positive about it, but the notion of using AI for security is as loud and as popular as ever, but you really have to dig through a lot of noise to find the true nuggets there. I do think the ability to do – previously, it was just pure automation that would let you do things better in security. Now it's really, you can think about it as super-smart automation. Let's really use the machines to do some reasoning about whether something is good or bad and then trigger some action based upon that.

If you put it in that context, I think the ability to for instance, to really recognize any mail coming into you and looking at all the factors around it; what time of day, who did it come from, what was the verbiage like within the mail? I'm pretty excited about understanding the natural language in the context of whether a Slack note or an e-mail to decide if it's something that you should be worried about or not. That's an example where you go from traditional pure statistics and automation to much more of a true machine learning approach.

[0:11:13.8] JM: How has the adoption of the cloud changed the world of security?

[0:11:19.8] SH: Another very good question. A lot of people obviously originally saw the cloud as risky from a security standpoint to sled to the growth of a lot of companies that did well, that CASB market in particular is an area that grew out of pretty much everyone realizing their employees we're using the cloud and having no visibility over it.

On one hand, I think you can argue the cloud is safer in many ways than running things in your own world. Certainly, if you go talk to the security teams at Amazon or Google or Microsoft, the amount of attacks they get on their infrastructure every single day is thousands of times higher than any single company. Likewise, the amount of technology and skill that they can put into their staff to prevent and protect and to get forwarding about these is better than any single company can hope to do.

In that way, it's safe in the sense that this is the – it is the aggregation of all threats and all skills being in there. I think that's good. On the flip side, it's very different for companies. You can move so much faster, you can do things from the bottoms up in the terms of a single employee going out and swiping a credit card to use these things. While it might be safe in its own right, the policies and what you might be putting into there and even how you use these cloud controls are not necessarily something everyone has trained on.

There has been a number of recent acquisitions and focuses on these tools that really help you enforce policies on the cloud for all your employees, even as they move faster and as they adopt them more aggressively. All in all, I'd say it's a mixed bag right now for those two reasons. Then the third one would be again, no matter what, even if you're in a cloud or anywhere, there's still a lot of policy decisions over who can do what, when should you encrypt things and so on, that thing.

You still have to have a security team that figures out what your policy should be there and actually implements them. That's been something where you've had to look at a lot of bigger companies having to hire people to do that. Or I think the ideal world is your existing security tools, you can create some policy and then have that apply wherever you're running, whether it's yesterday's mainframes, all the way to the cloud, to containers, to whatever else is next. I really do think that that's where we need to go is let's declare a security policy at some top level and then have it be instantiated wherever you happen to be running as a company.

[0:13:36.1] JM: Can you talk about that in more detail, because I hear what you're saying, but you have all these deployments where it's like, I'm an insurance company. I've been in business for 40 years. Only now I'm moving into the cloud and figuring out my hybrid architecture. The cloud presents a lot of great security properties. The fact that now I have this entirely new medium where I'm running some of my workloads, so some of my workloads are going to be on-prem, some of them are going to be in the cloud. It seems it actually makes security riskier, more complex, more detailed. I don't know. Tell me if I'm wrong, or a company that's moving into a hybrid architecture, let's say you're the CSO at that company, how do you get towards a place where you can have some uniform policy management strategy?

[0:14:28.6] SH: I think you're absolutely on to one of the big challenges. I would even abstract that after being in this industry for a while, anytime there's a new environment, anytime there's heterogeneity of some type, it does make the job harder for what you might have done before. The way I typically have thought about first cloud adoption and now secure cloud adoption, really the older and the more regulated a company is, the far slower they're going to be in moving towards this. They have too many entrenched processes. With regulation, they've figured out how to do something at least according to the regulators.

When I see that more traditional or mainline companies that have these restrictions, like an insurance company, they typically end up carving out at an entirely different team and they pick one specific small project. They use this team to show the rest of the company what could be possible. This follows a lot of the other things you cover, whether it's just we're going to be more agile, or we're going to move to DevOps, they always get this green team and they put people around it and try out something.

In that world, I'd say the security is very bespoke to them. It's very much focused on that one project. I think this is one of the huge opportunities is startups that can now come in and bridge from how you are doing something to where you go forward. I'm seeing some early companies do this. They might do this through orchestration processes, like let's create the if, this, and that type of scripts that allow you to push things out across the environments. It certainly is often the case that you have your cloud specialists that's now on your security staff and they're in charge of manually applying the process there.

Then certainly, both my own companies and seeing others that are really trying to have that message now too and really have the products where you can declare things once and then have them work multiple places. It's very hard and it takes a lot of plugins and all of that, but I do think that's where security has to go.

Again, if you go back in time, this is where every management tool company goes. They start best-of-breed for one environment, and then over time they add more and more environments into it. It's that heterogeneity that ends up making them really a popular for the much larger companies.

[0:16:37.9] JM: There are three different security environments that I'd like to get your perspective on for how they vary. One is that enterprise we just talked about, the insurance company it's been around for 40 years. Another is the brand-new startup. Let's say I’m a brand new startup, I'm one two three-years-old, I've got good traction, but I'm running as fast as I can, it's very hard for me to even think about security policy. I'm just trying to think about raising the next round of funding and keeping my customers happy, keeping the lights on.

The third category that I want to explore is these late stage cloud native startups. Maybe not exactly cloud native, but you take companies like Uber, Airbnb, Thumbtack, Netflix, where they were basically born in the age of the cloud. The people working there are super sophisticated, or many of them are. How do the security factors and security policies vary across these three types of companies?

[0:17:44.7] SH: Yeah. I love the couching of that problem. This again probably applies to almost everything you look at within the software engineering world, because every year there's a new better way by default to do things. The companies, obviously Netflix is a great example. Everyone knows how well they adopted Amazon Web Services and they put out a ton of open source to show what they've had to create along the way.

You see all these companies now that are at, I don't know, we call them preteens or something. I'm not sure where they live overall. They are hitting various bottlenecks and they're needing to re-architect their products quite a bit. I think certainly, in this five-year period now, it's the move to microservices and using containers for being even more lightweight and how you build these apps. I've seen a real growth not just in security, but everywhere else in terms of how do you take wherever we're coming from and break this thing into the right parts. and I think that applies to security as well.

I think you've seen and heard about people who take monolithic apps and break them into microservices. I see when they're doing that, there's typically some component of security built into it. Lots of approaches these days in terms of when you're deploying a new app for instance, no one actually updates the software and these microservices. They actually redeploy them from scratch with the latest software. That's one way to start fresh each time, which is a good security practice.

Oftentimes, you're seeing now in the zero-trust world this notion of identity associated with each of these microservices, and that's being built in from the start where there's encrypted and protected communications between them. Forgetting the technology piece, you also see that it's like Maslow's hierarchy of needs a little bit for software. When you're a first, second year software company, you just want people to use your software. Sure, it'd be great to be perfectly secure and all these other things, but no one cares if it's secure if they're not using the app.

You have a shifting of the requirements there. I always see companies when they hit what you said, maybe the three, four-year mark. It probably ties more importantly with when you're getting some more mainstream customers using your product. As a board member, or as an engineering leader there, you absolutely know that your risk now is like, what if we get broken into, or what if the data leaks? As opposed to what if the product doesn't work, or what if the user experience is terrible?

I just say both the need and the resources to do a proper job probably ramp as the company gets older. You always see it year two or three, or right before a significant launch they do their first bug bounty program as an example, or they boast their first pin testing thing. I think it's typically working that way.

[0:20:23.3] JM: I want to go deeper into the zero-trusts market, because you were talking about zero-trust at RSA. I can just imagine the football field of vendors that are offering various zero-trust solutions. I guess as a venture capitalist, what are the – obviously this is a trend, but many things are trends. You can't just say, "Okay, I invest money in the trend." What is the best way to place a bet on zero-trust networking?

[0:20:56.9] SH: That's a great question. The way I think about it is you need to know what's coming down the pipe and what is the problem area three years ahead of when it's actually there. What I see a lot of these big awareness campaigns, oftentimes are driven by the analysts who declare this is what your architecture should be, or this should be your priority for the year.

If you aren't working on a 10x better solution for that two, three years ago, you're not going to be ready for primetime when it comes out. I think of most of these trends has official either doctrine or marketing or things that are going on. Why it matters so much to these startups; one is at RSA, I think there are 800 startups there. If you imagine poor CISOs who are trying to choose what products to use, they're in non-stop POCs, proof of concepts, and they're really constantly trying to figure out who they should use.

When they start to hear things like, "Oh, I should be worried about zero-trust," and then they see the leader in zero-trust is this, that really just narrows down the field that they have to look at. I think it's super critical for really being a real product in that space just to get above the noise and to get to the priority list.

Also from a pragmatic standpoint, the way these big companies often work is they will allocate some chunk of money for each initiative. We're seeing right now a lot of companies have said for 2019, “We are going to spend 50 million dollars on zero-trust. It's a really important initiative.” If now I'm a company associated with and who's able to deliver a –

[0:22:22.7] JM: Sorry, is that a realistic number? 50 million in a year on zero-trust specifically?

[0:22:27.0] SH: It is for a big company for sure.

[0:22:28.8] JM: Big company –

[0:22:30.3] SH: Well, I’d say any of the Fortune 500 could easily spend that much. Now what falls under that, this is where budget games often come in. Certainly, you might have been doing something. If you can now justify it as zero trust as an internal employee, that's one way. Since the dawn of time, employees have gotten their projects funded. I think there's a reality to it too. It is something you say the analysts have spoken this really is a critical part for me to get right. I have a big budget and I'm going to put a big chunk towards it. The numbers are real.

Again, why this matters for the startups, it's often easy to go in and say, “I have this great solution that solves your problems.” If they're not pre-allocated saying this is an important initiative for us, this notion of a startup mapping to budgets that have been created is something we deal with every single day. It was something I wasn't super clear on how that worked until I was really deep into this. Going in and pitching a product that doesn't have explicit budget associated with it is so much harder than one that does.

[SPONSOR MESSAGE]

[0:23:34.6] JM: Hired simplifies the job search for engineers with a data-driven, personalized matching process. Head to hired.com/sedaily and create a profile today. By creating one profile, you'll be matched with over 10,000 companies looking for engineers like you.

Hired uses intelligent matching technology; data science with years of experience matching engineers with jobs. Hired also has a human in the loop. Hired gives personalized career coaching to match you with opportunities based on your skills, industry, interests and desired salary.

Create a profile today at hired.com/sedaily. Find a job that you truly love that is personalized to your background and your preferences. If you aren't an engineer, Hired also helps designers, engineering managers, product managers and other tech workers find their dream jobs. Just go to hired.com/sedaily and check it out.

[INTERVIEW CONTINUED]

[0:24:50.3] JM: How would you vet a company, if a company came to you and said, “We're a zero-trust networking company.” They lay out their go-to market strategy. What's an appealing go-to market strategy, or the inverse question, what are the red flags you look for in? Because the security market, for people who don't know is I mean, to my mind, it's quite different than some of the other software solution markets, because there's no network effects. There's much less word-of-mouth. It's more like, do you have a really, really good sales team? Do you have a really, really good integrations team? Do you understand pricing really, really, really well? Can you empathize with these really big companies that have really big budgets to spend and really good reasons to be concerned?

In that way, it's very different than some of the enterprise prosumer, Slack, SaaS, ZenPayroll solutions. I'm just trying to get inside your head as somebody that's assessing these companies that are coming through your door and saying, “We're selling, for example zero-trust solution.” You can look at these companies and sometimes be like, “That's a great engineering solution, but you are not the team that's going to be able to sell into the enterprise.”

[0:26:06.8] SH: Yeah. That is at least half of the job of a venture capital team is to do the diligence, or to do the vetting, or to understand which ones are the fit for what you're trying to accomplish. This is everything. I would say, security has some real positives in terms of how you do due diligence and how you choose which ones will be the – at least what you think could be the winners.

There's not an explicit network effect often, but in many cases there is so much of a following the leader approach in security. There's certainly well-known, if you're in banking and you see JPMorgan adopt something, that's already going to go to the top of list of something you think , "Wow, if it's good enough for them, I really care." For instance in the financial sector, there's a lot of talking between teams and there's a lot of job changes between teams. You do get a very nice networking effect following from that.

I think the other thing, what I do all the time and anyone who ever comes in to pitch an enterprise company to me, my first question is always explain how this is at least 10 times better than what they're using today. For me, that's an important question because of all the noise and all the things going on, being twice as good or three times as good just doesn't matter. From a technology standpoint, it has to be a sizeable jump forward. In security, it needs to be a sizeable jump forward in either the types of things that it finds, how quickly it finds them, how convenient it is to employees as they're doing it, the price. Something has to be that much better. That's really how do you distinguish yourself from the others.

In terms of domain specific questions, zero-trust I'm probably a bit more technical than a lot of the venture folks. I spend a lot of time understanding the area itself and some of the key customers, what they're talking about is their best solutions today. I do tend to go pretty deeply and say, "Okay, zero-trust is about trust no one, it's about individual nodes within your data center being able to be compromised, how do you keep it from spreading? Explain how this does that." I'll definitely look for them to explain how they do it, and not just from a technical standpoint, but really if they're pitching a venture capitalist, it should be the same as how they pitch employees to get them to join the company, or how they pitch big customers to get them to take a risk on a smaller company. That storytelling behind why this satisfies the tenets of this space you're going after is really important.

[0:28:25.1] JM: Is there any bet you've placed on a "zero-trust solution," yet?

[0:28:30.9] SH: One of my biggest bets is called Illumio, which is it actually didn't start being called zero-trust. Illumio is a company that I've been in for about five years now and they focus on what's called micro-segmentation. Really means carving up your internal network, so that only he pieces that are allowed to talk to one another can talk to one another.

When the company was started, the idea of trust no one was very much growing in the notion of east-west traffic in a data center being something that's not protected by today's firewalls and something we should care about. It would be –

[0:29:04.0] JM: East-west, that’s load-balanced traffic, or –

[0:29:07.0] SH: Oh, sorry. East-west usually refers to servers talking to one another within a data center and you typically call north-south is when they start talking outside the data center to customers. I don't know why it's – I don't know it's north-south versus east-west. It typically means inter-server communication as opposed to going through the public internet out down to other folks.

Anyway, the point was the notion that you shouldn't trust all these things speaking to one another internal to a data center and realizing that traditional firewalls don't reach inside a data center, they typically form that perimeter around it. That's why we got going on the company. It's been selling really well to a lot of these environments. I would say only over the last three years has it been called zero trust. Forrester came out with their wave product, which is where they look at these. Lo and behold, we’re at the top of that. We realized, “Okay, we are in the middle of this zero-trust wave.” Now that we're able to be well associated with that and legitimately delivering on it, the demand for the product has gone up substantially by people with budget for that this year.

[0:30:13.5] JM: Are there good open source solutions around zero-trust?

[0:30:19.2] SH: That's a good way to phrase it. There's certainly a lot of interesting open source projects that are then turned into use in an open source solution. I'm trying to think off the cuff. I can't think of companies, or open source projects that are explicitly zero-trust. I'll give you a couple of examples though. One company – I'm involved with them as well, so I'm obviously biased, but there's a very popular network open source project called Bro. We just named change the name to Zeek to be a little more – Bro is not cool these days. Actually, it was named after Big Brother, like the Orwellian thing, not after being like a bro.

Anyway, the core way that people really understand how networking traffic is going on within a data center. Again, super popular framework used by tons of companies as they built up their own solutions. Now that people are recognizing whether you're in the cloud, or whether you're local to your data center that everything is about this network traffic. It's now being rolled into new startups, as well as to do it yourself projects around zero-trust.

[0:31:21.8] JM: I imagine in many cases, the technology whether it's open source or not, may not even be as important as technology plus integration. You need somebody to Sherpa you through the integration, right?

[0:31:35.0] SH: The whole topic of open source is again, something you talk about all the time. It seems to matter a whole lot less insecurity than a lot of other spaces. Certainly, people like it and it always has the benefits of more transparency, the ability to take it and go do your own thing. Especially in security, I tend to find this mostly in security and maybe some of the management tools, like people just need this thing to work and they want someone accountable for it to work, whether you do that as an open source or not, I think is probably secondary. I would say, I've never done the study. I should. Of the 800 companies at RSA, I don't think of a lot of them as being pure open source plays at all.

[0:32:12.8] JM: You think that'll change? You think the security tools will be more open source over time? Because I mean, you think about something like Linux or Bitcoin, these things have been hardened by virtue of all the eyes on them, but you need to pass a certain threshold of the number of eyes. When you're under that threshold, your product is more vulnerable by being open source, because you don't have enough eyes to find all the security holes. Once you pass that threshold, you've got eyes over every minutia.

[0:32:40.4] SH: No, that's a really good point. There should be some – you can name a number, that's the number of eyes that have to be on something for it to be safe. I would make a distinguishing between the other core platforms people are using and those being open source tends to be a preference, because of all the things you just mentioned; certainly, transparency. I think people think of vendor – more vendor control by being able to take your code and run if you need to. I would say the things that people are running on are definitely preferred to be open source in many cases.

There's the eyeballs factor, but where oftentimes things fall apart on the longer tail of open source projects is when great, you found the bug, who's going to fix it and who's going to get it into a rolled up distribution? In that case, open source can be challenging. Again, these are for the longer tail of packages that might not have a big company behind them. If you don't have someone to fix it, then you own the problem. In that sense, you'd rather have a commercial entity, or closed source or something like that.

We're actually involved with a cool company called Tidelift, which is trying to match up developers with their open source projects, in part to guarantee that there is someone who can fix these security issues when needed, recognizing that challenge for some folks. Again, the security projects themselves, so much of security is a lot of things integrated together. A lot of the tools for stitching them together and the integrations have open source components.

I think there's the overall security solution versus individual projects that are getting together, even just – one example is the sim area. This is where all of the events come in to a security operation center. This is dominated by folks like Splunk and Sumo and ArcSight and all these companies that are out there. I don't think anyone's ever thought of those as being open source or need to be. There's part of your security solution that just has to work super well. There's probably a distinguishing factor across the platforms that you're running on that need to be open source for various reasons versus the core tooling within security.

[0:34:36.8] JM: Let's talk about malware. Describe the modern malware that might threaten an organization.

[0:34:41.9] SH: Boy, that's the best question right now. Malware is bad software basically, something that comes in to cause mal intent. For those who have been around for a while, it used to be that Windows exe file that you would open up, people don't really talk about that much anymore. The traditional virus checker sitting on your Windows desktop is still matters, but it's not really the dominant factor.

Today's malware is coming through a lot of different mechanisms. Some of the scariest stuff is being delivered just through the web. There's plenty of cases of JavaScript that has been embedded somewhere that can infect your machine somehow. What's scary about it, phase one of the internet was recognizing sketchy websites versus normal ones. A lot of companies were built up categorizing websites into known dangerous, or unknown or good. You could choose where you go or not. You know not to click on some things that look like skull and crossbones on them or something.

What's been interesting as of the last five years is malware's being delivered through things like the ad networks. You might trust cnn.com, but the ad network delivering you ads on cnn.com is coming from a totally different point, so there's all these different sites that are aggregated on that webpage. It's become very difficult to know which ones are coming in in a bad way. Web-borne malware is increasingly scary and has led to a lot of tricky new problems.

Then another one, certainly right now you're hearing more and more about document-borne malware, so something that might be embedded in that PDF file that you open up. Having to really rethink, even if it's coming from a trusted source is there something in the macros that are written in this excel document or something like that that could cause trouble. There's just so much power in these documents now that we're seeing that as another frontier.

I think mobile devices people have talked about for a long time. I still think that's proven so far to be far less dangerous, mostly because of the operating system control and how much is locked down. A lot of what I've been focusing on over the last few years now has been what are the solutions for web-borne and document-borne malware.

[0:36:52.7] JM: I'm surprised what you say about mobile devices, like if I was running an enterprise and I had my employees using, or looking at sensitive documents on their phone, which everybody does, and my employees are installing flashlight apps on their phone, don't I have cause to be concerned, or are the operating systems like Android for example, iOS obviously a more secure story, but if they're using Android phones, I mean, don't I have cause for concern?

[0:37:21.9] SH: Certainly, you could and there's definitely a lot of examples. In the cases of the famous flashlight apps, more of the damage to date has been done. I guess, you could definitely call that malware. It was in a different context than what I was thinking of. The damage of the flashlight app on almost all these cases has been a bunch of your location data, or your own personal information on what all apps are running on your system, or maybe where you've been that was being transmitted to the companies.

I was putting that under the privacy breach standpoint, but it is a form of malware. Again, I do think there are certainly classes of problems here and people could be concerned by them, but I would just say in general, that has not been the battleground yet that I think some of the other areas have been. Again, it's largely because of even I think everyone thinks of Apple is stronger on the security controls. Even that on the Google side, the ability to take apps out of the Play Store if they haven't – if they've gone bad and really the sandboxing that happens between apps is far stronger than it is in some of the traditional operating systems.

I think everyone over the last 10 years, the number of companies that have launched around being worried about various virus attacks of different sorts on the mobile has been large, but none of those have been particularly large compared to what's going on in the rest of the world.

[0:38:36.1] JM: If I install really malicious malware somehow, either through clicking on a PDF, or I'm surfing the web at a lunch break and an ad – in an ad network on CNN manages to infect my computer, what's the worst that can happen?

[0:38:54.7] SH: These things can follow a lot of different mechanisms in there. It's incredible programming that goes into these things used for bad, but the amount of technology there is so high. Yeah, I would say a traditional approach to malware might be for a very clever malware, it might be somehow it gets onto your system. Typically what that means is there's some application or process that is now running on your system that has privileges of some kind.

In the ideal world, this malware has become the most powerful user on your laptop, or on your server. It's a super user of some sort. In the less powerful case, it is running as you. It has the same privileges to access files, or to go places that you would have. All of them find some way of being run on behalf of either the user, or the super user of that system. Then once they are in that privilege, they have all sorts of mechanisms for evading capture and it is a cloak-and-dagger game. Oftentimes, they'll go quiet for months on end. They won't do anything. On a certain date or after some certain time, they'll then wake up and they'll do bad stuff.

Even the bad stuff that they do is cloaked in an amazing set of tricks that people have used over time. This process itself is not something that you can just see running. Or if you are, it's going to look like something that's innocuous. If you're tracking is something and download 50 gigabytes one night, that might be something to look for. Most of them are not that dumb. They'll trickle out little pieces of data at various times, again time to be evading capture. It comes in all these different forms, but at the very core it is usually about how do I infect this machine and get some privileges?

It's absolutely about how do I then spread to other machines that this person might have access to. Then it becomes once I'm in there, how do I get data of some sort back to mission headquarters basically.

[0:40:46.8] JM: We had a show recently about cryptojacking. Have you heard of this?

[0:40:50.2] SH: Yes. I've seen quite a bit of cryptojacking. It's an interesting one in its own right, where I guess you covered – they basically encrypt some of your files and say if you don't give me some Bitcoin, you don't get your file.

[0:41:00.6] JM: Well, that’s ransomware. Cryptojacking, maybe that's also classified as cryptojacking. The cryptojacking that we did a show on, or at least the way I hadn't heard of this term before I talked to this guy, but it's basically the JavaScript mining Bitcoin in your browser.

[0:41:17.8] SH: Oh, yeah. I think of both in the crypto hijacking world, but certainly two different ones. That's a form, rather than actually to put them in context. In the case you're speaking to, definitely is one that we've seen a lot of. It's particularly interesting in the cloud case where if it gets into your system, rather than sending data, like the value being the data, the value as being computation time that's charged to you. In that case it's like, I don’t know if you ever use SETI at home or something like that, but it's the way to do computation and try to earn you some – earn some Bitcoins. I think the ransomware is another form of that, but yeah, this is a particularly prevalent use case that's hitting now where people are finding lots of stuff running on their behalf.

[0:42:00.1] JM: Yeah. Have you seen any startups get slammed by ransomware, or is it just those big stories that you hear, like the hospitals and –

[0:42:06.4] SH: Ransom ware has been super popular in the sense of hitting big and small companies. It's just the data matters a lot more typically in an older, bigger company. It is an interesting side effect, but most of these data kidnappers essentially have had to write really great tutorials on how to buy Bitcoin, because if they're trying to get ransom this where and people don't have it, I think that was funny. If you ever looking at how to get started with Bitcoin, some of the best tutorials, they're coming there.

What's interesting for me, what I hadn't realized I had a very large company doing data backup and data recovery and people have always done that for if my system crashes, how do I go back in time? I've definitely seen that as the dominant growing use case has been, "Okay, I was hijacked at 2:00 p.m. on Friday. Let's go back to 1:00 p.m. on Friday and forget that ever happened." You can actually recover your encrypted files by just going back in time.

[0:43:05.1] JM: Yeah. The cryptojacking on the side of the mining Bitcoin on my computer, is this is a – is it a unique threat at all, or is it just – do you lump it under the same category as malicious ad network delivery? Anything new about it?

[0:43:23.4] SH: I don't think it's new. Like I said, at some point the whole point is to take value out of the system that you've attacked. I think the value comes in a lot of forms. It might come from personal data value that then gets sold on the black market. It might be some file it finds on your system, or it might be computation time that it just stole from you. I think all those are a way of taking value out of something once it's been attacked.

[0:43:48.0] JM: One of your investments – I was looking at this company. It was pretty interesting. Menlo Security. Explain what Menlo Security does to deal with malware.

[0:43:56.9] SH: Yeah, this has been a really fun company for me too. This is my first series A investment when I became an investor. What they do is they provide a form of isolation for the web and for documents and for mail. When you think about the big picture of security, I really think it changed – I think everyone thinks a big change has to happen.

The traditional word of security has been how do I detect some bad thing that's happening and then don't let it happen, so there's signatures and viruses, firewalls might do some little simulation or look for things, IDS systems are doing this. If you really think about it, how well has this really worked for us?

Certainly, you take 95% or something of the known attacks from ever getting into your laptop, or to your servers. Whenever there's a day zero attack, some new type of thing that it doesn't know about, it often fails at catching it. I think a way to think about the security world changing is let's do all that, but let's also really focus heavily on preventing damage from really spreading once it gets in.

That is a form of zero trust a little bit, but I wouldn't call it that. I just call it isolation. Minimal security, rather than run a web browser entirely on your laptop, they've done this really cool approach to running part of the web browser in the cloud. It's actually the part that touches the dangerous JavaScript that could be coming in. They very quickly and very seamlessly do all the execution part of a webpage in the cloud and then mirror what the webpage looks like and how it feels to interact with it down to your laptop.

You have no idea this is happening and that's critical for people to adopt it, but what it means is the bad stuff, even if it's there, it's running in some container in the cloud and you just throw it away at the end of a session. As opposed to in the old world, it would have been running on your laptop and left some vestige there that could cause damage.

In many ways, it's a form of virtualizing webpages in that particular sense and isolating them from causing trouble. This company's taken off really quickly and is selling to some really large customers who are basically tired of the cat-and-mouse game in security and saying, “We're going to keep doing that, but if you can promise me I'll never get infected from a webpage, why wouldn't I move to that?” That's exactly what they've done is if you never have the executing piece get to your laptop, it's never going to cause a problem.

They've subsequently extended that solution into e-mail, so that you can't accidentally click on a bad document, or a bad link and even into documents, so that even if you're interacting with a word document, or a PDF document, the dangerous part is running in a disposable cloud container while the user experience has no idea that that's happening. A really interesting company and I've been excited by the more general thesis around isolation as well.

[0:46:42.1] JM: Yeah. I found it pretty clever too. Basically, you render a webpage virtually and then you deliver as I understand it like just a shim of that webpage to the actual user within the enterprise, so the user just sees a virtualized browser where the functionality and the vulnerabilities are sandboxed. Am I understanding that correctly?

[0:47:08.1] SH: That describes it very well. I think there's two really important points to this. The first is that there's something in web browsers called the DOM. The DOM is it's the perfect layer to do this at, because a DOM is universal across browsers and I learned this at VMware; if you can find the right layer to virtualize and get in it, a lot of good things happen.

What this means is basically every webpage is going to work and it's going to work to every type of browser, because we picked this DOM layer. As you said, this shim approach is a good way to think about it. Had to say this from the start of the company and we've had to focus on this. There's always this challenge between security and convenience to a user. As they always say, the safest system is not connected to anything, but that's not realistic.

What we had to spend several years doing is certainly that core DOM virtualization pieces there, but if you still can't use all of your plugins and can't drag and drop and have some weird file upload. If anything looks different to a user, they're going to find a way around Menlo Security. That's what we've done I think a really good job of is making it seamless to the user while making sure it's protecting everybody.

[SPONSOR MESSAGE]

[0:48:24.5] JM: Failure is unpredictable. You don't know when your system will break, but you know it will happen. Gremlin helps you prepare for these scenarios by testing how your system responds to duress. Gremlin provides hosted-chaos engineering as a service, drawn from techniques pioneered at Netflix and Amazon.

Prepare your team to prevent disasters by proactively testing failure scenarios. Use Gremlin for free by going to gremlin.com/sedaily and find out how Gremlin can fit into your software development process. The first time I was at a company that dealt with an outage, I was terrified. I was at a stock trading company and NASDAQ, which is the second largest stock exchange in the United States froze up. This was a bizarre outage, but we had to deal with it.

You will have unique outages at your company. Maybe the NASDAQ will freeze up and you'll have to deal with it. The best way to harden your infrastructure to be ready for those stressful events is to put stress on your infrastructure today.

Go to gremlin.com/sedaily and learn about the different ways that Gremlin can chaos test your infrastructure. Max out CPU, black hole or slow down network traffic to a dependency, terminate processes and hosts. Each of these shows how your system reacts, allowing you to harden things before a production incident. Checkout Gremlin and use it for free by going to gremlin.com/sedaily.

Thanks to Gremlin for being a sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:50:16.2] JM: When you look at that solution, that the virtualized browser, to me that seems like a great technological solution. It seems like something that could be copied, it could be re-implemented. When you look at a company like Menlo Security and you're evaluating the technical solution, do you see a moat there, or does there even need to be a technological moat? If they get out ahead of the market, they can be – the person that sells to JPMorgan and then the rest of the dominoes fall to other customers, is that enough to get out ahead of the market and it doesn't really matter if some other secure – some established security vendor with other go-to market channels just copies their solution? Does it matter how replicable that solution is?

[0:51:05.6] SH: That's something we talk about every single investment is what is the protection, what is the moat as VC speak for how they're protected in this world? If you didn't invest because some big company could replicate something, you'd never do anything. You always have to look at what is the unfair advantage for this firm. In the case of Menlo Security, we were working on the product for two and a half years before anyone even heard about it and in that time had hired a lot of the best engineers thinking around this. We actually license some key patent work from Berkeley. We actually created a lot of our own patents. You never say a company's protected because of their patents, but it's an important part of the process.

It's often about how do you accumulate the engineers and really go all in on the solution and think through all the problems to stay ahead of people. Then at that point, it certainly becomes your brand. Is a JP Morgan using you so that others might recognize that? You just have to continually stay ahead at that point. Early on, it's about the team, the technology approach. Then the case of a lot of companies, a lot of the existing firms out there can't afford to go all-in on a solution like this. They might have vested interests in the detection phase, or they're more interested in categorizing websites than just isolating all of them. We continue to see play out right now, where I think anyone who thinks about security for a while realizes isolation needs to be a bigger part of it, but they have other things going on so they just can't be single-mindedly focused on it like we are at Menlo security.

[0:52:35.5] JM: You mentioned Berkeley. Academic security research, I mean, most major computer science institutions have some academic security research. What's the life cycle like, or how frequently are research endeavors productized? Does that happen on a regular basis?

[0:52:57.9] SH: It does across pretty much every industry. I wouldn't say that security is more or less than any other. I personally worked on VMware with my advisor at Stanford before creating the company. It was an academically created firm. Yes, Mendel Rosenblum was the professor there.

[0:53:15.2] JM: Oh, wow. You worked with him as an undergrad?

[0:53:18.7] SH: I was there as a grad student. He was my PhD advisor.

[0:53:21.4] JM: Oh, that’s cool.

[0:53:21.9] SH: His wife is the founder of VMware, Diane. The point was that was a very – started as a very academic project, which is really meaningful to me, so I'll speak for a minute about it and we can go off later. One thing I really love about academia is that they have the time to step back and look at history, or look at everything going on before coming up with a theory and then going after it. I think you get really thoughtful projects that go into this.

In terms of productizing it, especially for an enterprise market that's not something that academics do particularly well. You typically pair up the idea generation and the thoughtfulness around where this fits with people who are ruthless on schedules and quality and integrations with other tools, things that you just don't think about in universities. I think it's very potent combination to take those two and feed them together. Oftentimes, what VCs do is we're meeting with professors at universities, seeing which students are graduating that have been working on some idea and then pair them up with some very enterprise-focused people that have done the company side before.

[0:54:26.8] JM: Does that happen to this day, or have the major companies cannibalized the research process?

[0:54:34.2] SH: It happens. Probably this week it will happen. It's a very interesting world. Whenever you talk to professors and universities, certainly there's – especially around here, a lot of professors will take a sabbatical and themselves go do an interesting company for a year. That's been very interesting to watch. It's the only place on earth where the workforce basically turns over every few years. The number of hot, sharp graduates students coming out of these popular labs is endless, and so that leads to a really a lot of good ideas coming out and a lot of company founders coming out.

[0:55:06.7] JM: What are the security companies that have had the biggest investment outcomes across the industry? What are the homerun, legendary security company investments?

[0:55:20.1] SH: There have been a lot. I think probably if you were to ask anyone today, they would say Palo Alto Networks looks like one of the biggest. I actually checked their market cap exactly lately. Yeah, they started as a classic venture-oriented company and now they're quite large and doing lots of acquisitions and have a big market cap. You can go through the history of security companies and there have just been a large number going through. Checkpoint was probably one of the earlier ones that everyone talked to.

As you go forward now, Tanium for instance is one of the largest security companies – private security companies by market cap. I think just any other part of the venture world, there's been every few years a very large multi-billion dollar company gets created. I'd say what's a little different about security is that there's a surprising amount of consolidation and a surprising amount of M&A that goes on. I don't have the data in front of me, but I believe more companies probably get consolidated into this market than they do in a lot of the other enterprise spaces.

It's partly because customers as we're talking about, they're so busy and they have so many types of solutions they should be looking at. I think more so than other spaces, security they'd love to have one or two vendors that can just give them a ton of the protection across all these spaces that they need. Because the types of protection needed have changed so much and get so broad, that means you need to buy yet another new solution if you can't generate it yourself. Versus a lot of other areas, I'd say there's not a lot of huge, huge cyber-only companies that are out there. There's a lot of midsize ones that have done really well and continue to grow through acquisition.

[0:57:02.1] JM: Is it an industry where acquisitions work more frequently? Because that's often talked about, "Oh, the acquisitions just don't work usually."

[0:57:12.2] SH: I think in this space, it works better than most. Again, if you start with the customer, they would love to have a fewer number of vendors where they can buy a lot of their stuff from. That's phase one is at least there's one vendor who can show me what I need to care about and that I can interact with one salesperson and do one contract. There's that part of it.

If you really want to talk about how companies come in and get better, it's when the products work better together, if they have a common user experience, if you can do one support call and get them all supported. I think in the security space, maybe the bar is so low for tight integrations of the products that they can afford to do it more easily than some of the other areas.

[0:57:53.4] JM: Those homeruns that you mentioned like Palo Alto Networks, any commonalities you can draw between them, like stuff about the founders, or their go-to market strategy? Or is it just totally hard to –

[0:58:09.2] SH: VCs are known for looking at a success and figuring out the pattern, usually a pattern of one or two, so everyone will attribute them to different things and you hear some really funny theories on great companies are founded by this or that. I think the way that the path always works is that they have a killer team. Killer team typically means like a great technologist, coupled with a enterprise team that is very well-known and they've done this before. That's part of it.

I think every wave of computing creates another set of really big companies. It's the company who ends up being the best at something. Maybe it's zero-trust right now. They use that wedge to get into all of the big accounts and to be very trusted. Then typically through M&A, they will add other things to their solution. Some of them have built them all themselves, but typically you'll see this really nice, sharp web, they happen to be in the right place at the right time with a killer solution. Then it really expands from there to take on all the other stuff on people's minds. Then you see that pattern over and over. It's a matter of how do you catch the right company at the right time.

[0:59:16.3] JM: Let's say you invest in a company, new portfolio company, they're trying to figure out their pricing strategy, what advice do you give them?

[0:59:23.0] SH: Great question. That happens all the time. Typically, what you'll do is go through a series – the way almost all these companies work is you try to find a few early friendly customers. These customers are someone who has that problem or they've identified it and they're willing to work with you pretty closely to make your solution satisfy their needs to integrate the right way, to present reports the right way.

Phase one of these companies is almost always about that, is finding some nice, warm customers early on. A critical part of that is how do you think about the value of this product, meaning how valuable is it to you and how would you see the value growing? Some things like a virus detector, you think about each laptop that uses it is incrementally safer. You're probably going to charge per laptop for that thing.

I think it might be in the case of Spunk, they decided that the amount of data that you throw into the system is the unit of value that you're going to keep thinking about, and so they charge by how many gigabytes of data you have in there and it grows and grows and grows. It's trying to first understand how it scales on that front where the value is. Then there's just a realistic thing too. If you want to get into companies and you have an enterprise sales model, meaning individual people who are going in and doing that more heavy-weighted type of sales, there has to be amount of value ascribed to this product to even afford that. If you can't make a $100,000 to $200,000 from a company early on, a bigger company, then you know you don't have the right product, or the right model.

We typically look at it from the customer backwards, as well as what can this sales model afford, then you do it obviously in different orders depending on what's going on there. If you can't afford to have a product that goes with an enterprise sale, there has to be a deep viral effect between these where needs to be loved by developers from the grounds up, so that you can get into the companies. This is a lot of what you spend time in basically between a Series A and a Series B investment in venture capital speak.

[1:01:28.9] JM: Have you met any companies that are trying to address security in the self-driving car space?

[1:01:34.5] SH: There are a lot of companies pitching themselves as security for I'd say at the top level, security for IoT is how they would put it, the Internet of Things as this giant moniker refers to. Some of them pitch it generically, saying the Internet of Things has these different traits associated with it. We're going to provide you protection. Those are pretty almost always off the mark, because it's such a generic statement. Then the smarter ones will say, “We're going after a utility grids, or we're going after autonomous vehicles, or we're going after whatever the next thing might be.”

There are large number of them out there, I will tell you that. They all have different approaches and they all have different thoughts. In the negative case, there's a lot of companies that haven't ever dealt with cars before and they just – there's a problem that they think is there and they're trying to figure it out. My personal experience has been whether it's in the security space, or the next Lidar, or some other thing for cars, people who don't really understand that market are really surprised later on when they find out the margins that are required by car companies, the need for dual sourcing on almost everything. There are a lot of unique things about that market that would make a naive new company hit troubles when they go after it. I do think it's something that will be important, whether it's something a Silicon Valley startup can satisfy as TBD.

[1:02:55.3] JM: What are the biggest vulnerabilities in the hardware supply chain?

[1:02:59.5] SH: That certainly has gotten a lot of attention, hasn't it? It's also raised alerts on how to do – I guess, how to do reporting in some cases too.

[1:03:06.7] JM: Sure. Oh, yeah. Reporting, geopolitics.

[1:03:10.2] SH: Well, it’s certainly something I'd say whether it's hardware or even software, where the software came from or where the hardware came from –

[1:03:16.4] JM: By the way, reporting you're referring to the Bloomberg article?

[1:03:18.6] SH: I am in that particular case.

[1:03:20.5] JM: We don’t know what happened there, do we?

[1:03:22.5] SH: There's certainly plenty of rumors that have gone around. I wouldn't spread them, because I would probably be causing even more problem. Certainly, the idea of something –

[1:03:27.8] JM: Dang. You can’t say anything?

[1:03:30.1] SH: Well, they'd all be rumors for real.

[1:03:31.7] JM: What's so weird about that article is – so it was this – for people who don't know, it’s this article that was about this problem in the supply chain with servers that were in Amazon data centers, in Apple data centers and a bunch of places. Apple denied it. Amazon denied it. It was very strange, because Bloomberg is usually quite on point with their reporting. Then what was super weird about it, and maybe I'm just – maybe I didn't see it, or I wasn't following close enough, but after a while it was just silence. No resolution. No follow-up from Amazon or Apple or Bloomberg or anybody, which is – am I describing it right?

[1:04:12.4] SH: Yeah, you are. It's one of the weirder cases there. I mean, from my perspective too, this is one of the geekiest things that's ever hit mainstream press.

[1:04:20.0] JM: Right. Yeah.

[1:04:20.3] SH: It’s always exciting.

[1:04:21.4] JM: Good sign for us.

[1:04:22.1] SH: Exactly. I think from my perspective, folks like Amazon and Apple had proven to everyone that basically, it's irrelevant and it's not a case for them, and so it went away. That's how I perceived it from the outside. They'd done sufficient debunking.

[1:04:37.1] JM: Okay, you don't see black helicopters?

[1:04:38.6] SH: I don't. I don't. I'm not in that world as much. I mean, I think you can talk about journalism all the way through. The rush to scoop something and to get it out, versus maybe the amount of diligence on sourcing of the data and confirming has been an age-old challenge, I think for any type of press. This is such a political time and conflict with China and whatever else, I think made it even juicier to try to get this thing out as quickly as possible. There's probably some truth there some examples within there that are relevant, but not at the level that was exposed. It's typically some gray area that's in the middle.

On the positive note for security, I do think it raised even to the next level the level of awareness over the supply chain dangers and attacks. Coming full circle to where we started, this is a form, it’s sort of the supply chain form of zero-trust. It's like, trust no one, or at least find a way to verify that this chip didn't have weird stuff put into it, this firmware doesn't have some hacking code in it. It's very serious issue. I personally been on the side of Apple as a supplier, where the amount of diligence they go into understanding not just your technology and what you do, but your human rights, everything about a supplier is so high that they've raised the bar on what you need to do there.

I think more and more companies will get to extreme certification of their supply chain. If not directly, then it'll be through their – whoever their integration partner is, or their distribution partners will be held to that level of accountability. Yeah, there's lots of tech solutions that are in there for this supply chain checking, but I think the scrutiny will be raised everywhere based on this and things like this.

[1:06:21.9] JM: Do you have a perspective on this Huawei thing, or can you give me any uniquely Steve Herrod perspective on what's going on there, or the optics just too unclear?

[1:06:34.0] SH: I would say, I've been involved with a number of government contracts over time too. Certainly again, the level of scrutiny and worry about supply chain attacks is very high. I think it'd be impossible not to at least put this in the context of China-US tensions and perhaps being part of the things at the bargaining table as you go through and do more of the trade agreements that we're doing right now. I will say it's certainly the case that telecom gear, or server gear, or networking gear if it is hijacked, then it certainly can cause all sorts of risk to whomever is using it.

[1:07:05.4] JM: You may not be well-versed in this, but do you have a sense for ways in which the Chinese tech ecosystem is misunderstood?

[1:07:14.5] SH: Maybe I'm not as expert as a lot of people, I'll just say the two things that we talk about quite a bit. I have a number of colleagues that are focused on the Chinese market a fair amount, and so at least through osmosis I'm thinking a lot of it. I would say at this point in time 2019, I think people have recognized that by them being even more mobile first and more internet users over mobile, they really push the envelope on the apps for mobile that are being used so heavily. I think everyone knows about a lot of these solutions that they're using for payments, or videos, or entertainment of different sorts.

I think in many ways, we can look to China for where is the mobile app ecosystem going. In general, it's considered as much of a leader on the enterprise side of the world. You don't see as many besides things like Huawei, or some of the gear side. We haven't seen as many innovative enterprise apps, or open source data projects, or that thing coming out of China. We see it in that world right now.

[1:08:12.5] JM: How does security concerns of governments compared to those of enterprises?

[1:08:18.7] SH: They're obviously very sophisticated buyers of security software. Certainly In-Q-Tel is a funding agency on behalf of the four-letter, three-letter agencies. They're able to be very thoughtful. We work with them on a number of cases where they can say, if you're going to be used by the government, this is how their whole value proposition works. We will invest some in your company and we will help you understand what it means to sell to the government. That's very helpful for startups who've come out of here and don't know what that means.

The things that you do have to go through, I think there's a lot more scrutiny on – I mean, they have some very sophisticated users who can audit source code and who can really understand what you're doing and who will really exhaustively certify and test the software through a bunch of different mechanisms that are there. Not to mention, they have scale requirements that are very different from a lot of enterprises. The size of the government, the amount of data they have really triggers it. I think they're a sophisticated user. If you can sell to them, you see a superset of what's required to sell to enterprises, which is nice.

Back to just the more geopolitical part, it is certainly the case that they care where your engineering team is and they think about that quite a bit. If you have a Russian engineers on your security team, you're likely not selling into the US government for instance, probably vice-versa as well. I would say location of engineers becomes a much bigger issue in that world than in a lot of the other world.

[1:09:40.9] JM: Speaking of which, what was the thing that happened with Kaspersky Labs a couple years ago, where basically the government – the US government said we cannot use Kaspersky Labs for anything? Do you remember that? What's the postmortem on that?

[1:09:56.0] SH: Well, it's probably similar to the Bloomberg postmortem, in the sense of it ran out of people following it in the news. It's a case where it's exactly the same thing as this supply chain side of things, so just happens to be it's more software-oriented and perhaps based on where the company is from. Just knowing that if you have this software on all your laptops, or wherever it might be and you don't fully understand what it's doing, then it could be a source of malware, or a various spying attacks. It's not much different from these other cases. I don't know that I ever saw the smoking gun proof that it actually was doing something bad, but the fact that they're saying we don't trust this in the government was enough for their purposes.

[1:10:36.7] JM: Do you follow the geopolitical side of cybersecurity that much? Or are you mostly focused on business enterprise side, or is it all the same?

[1:10:46.3] SH: You have to be aware of it. What's been particularly interesting over the last 10 years is that the number of attacks coming in, first of all it was individual hackers. Phase 2 was maybe teams of hackers. Phase 3 was organized crime, like pretty significant organizations. Then phase 4 is definitely the nation state attacks and it's very well – it's been very well covered where these things are going on.

What's more a lot of companies have to focus on what's going on attacks worldwide, so that they can be smart about what to protect their customers from. I have one company that's job is to look at threats around the world and you see the cool maps of – they're not cool, but it's showing, like right now North Korea is attacking Japan and this is a type of attack they're doing. You would track that so that you could say, "Hey, this is a type of attack that might come to you mister bank customer in the US, or London."

I think the ability for the teams to be attacking from anywhere in the world is certainly huge and very important. The ability to get knowledge by watching what's happening around the world becomes very important as well.

[1:11:52.2] JM: Now, there's a narrative that in China there's a much more porous relationship between the tech giants and the government. In the United States, it seems like – I mean, even Snowden revelations aside, there is a pretty porous relationship between the tech giants and the United States. I mean, you have Amazon GovCloud, you have heavy lobbying efforts. I guess, it's less of an open secret, or may it's simply – it is less porous, but do you have a sense for the broadly speaking, the level of intimacy between our tech giants and the US government?

[1:12:34.0] SH: I would say that one thing in the news lot these days has been the push back of software engineers from – or the more liberally-minded engineers that are at a lot of the tech giants as they get used for perhaps as they're being considered for use in a military use. I think we've seen that a lot in Silicon Valley, right or wrong we've seen that. I mean, historically it has been government funding often for defense that's led to so much of the big innovations. Obviously, the internet and many other cases like that.

I sense if I were to categorize it, I would say it's definitely less integrated as it is in some other countries, or maybe in the China side of things. I think there is a certainly a tight tie between them. I think again, you often push the envelope with many government use cases, than then can be used for a lot of other customers.

[1:13:23.0] JM: You're alluding to things like Dragonfly and Maven and maybe like Amazon recognition. I find some of these cases so strange. I might get criticized by the audience for this. I really want to do a show with one of these engineers that has criticized Maven, or criticized Dragonfly, because they come down – some of these engineers come down so strongly, like they know what they're talking about. To me, both the cases Maven and Dragonfly seem very subtle, very subjective.

On Maven, the help with I think identification of humans by drone, there are plenty of ways that can be used to save lives that are completely not going to kill people. Same thing with Dragonfly. If you give Chinese dissidents access to better searches that may be surveilled, is that strictly bad as a human rights technology? It's not clear to me. The lack of subtlety with which these protesting engineers are approaching this issue is disappointing, right? Speaking as an engineer that is trying to bring a dialogue to some of these kinds of issues, it's like, grow up. How did you get a job at Google if you don't have the subtlety to discuss these kinds of issues? Do you disagree with that?

[1:14:50.6] SH: No, you should have the Software Engineering Daily political edition.

[1:14:52.7] JM: I need to.

[1:14:55.4] SH: My personal opinion on this is that these technology changes are coming and they will be used in some capacity. Personally, I think if you can get involved with their adoption and put in those safeguards and understand the risks and the challenges and address those, that's far better than just closing your eyes and pretending this isn't happening. I'm more of a fan of engaging, but being really smart about how you do so and trying to do what you believe is right within the context of openness and discussion and debate.

[1:15:23.4] JM: Yeah. What's your biggest request for startups, for people listening in the audience?

[1:15:28.8] SH: That's a great question. I guess, I already leaked. Whenever I meet a company, I really want to understand why they're at least 10 times better than anyone else and not two times. I think if you don't understand that, or don't think about it, you might question is this really the endeavor I want to take on? Think big and think bold, or go do the project under the bigger umbrella of some other company. That's probably where I end up passing the most is when I don't see something as being much more than just an incremental change.

I personally come from a far more technical background, so maybe different from a lot of VCs. I like to really go into the weeds pretty quickly and understand the tech team that's there and their chops and how they solve problems. It's geeky maybe, but you should expect that from me if we meet.

[1:16:13.9] JM: Preaching to the choir. How is General Catalyst changing as a fund?

[1:16:17.6] SH: It's been fun to be here. I've been here six years now and the fund has grown first of all quite a bit in terms of how much money we are fortunate enough to have to invest.

That's been due to being involved with some really cool companies and having some good early results. It's a lot of fun here. We're in New York and Boston and San Francisco and Palo Alto where we are right now. I think that's been really key for us.

You can't really do startup early Series A startup investments. I don't think you can do it well, unless you get to see the team every week, every couple of weeks and hopefully adding value when you're seeing them. I like all of our team being near where a lot of the founders are and really diving in deep. That’s great. It's really great to be here and it's a fun time to be in venture too. There's just so many changes happening at all times. The fact that we get to meet interesting companies all day every day is such a pleasure.

[1:17:10.8] JM: Steve Herrod, thanks for coming on the show. It’s been great talking.

[1:17:13.1] SH: This is fun. Thank you. We should do it again.

[1:17:14.8] JM: All right. Yes, definitely.

[END OF INTERVIEW]

[1:17:20.0] JM: This podcast is brought to you by wix.com. Build your website quickly with Wix. Wix code unites design features with advanced code capabilities, so you can build data-driven websites and professional web apps very quickly.

You can store and manage unlimited data. You can create hundreds of dynamic pages, you can add repeating layouts, make custom forms, call external APIs and take full control of your site’s functionality using Wix code APIs and your own JavaScript. You don’t need HTML or CSS.

With Wix code’s built-in database and IDE, you’ve got one-click deployment that instantly updates all the content on your site. Everything is SEO-friendly. What about security and hosting and maintenance? Wix has you covered, so you can spend more time focusing on yourself and your clients.

If you’re not a developer, it’s not a problem. There is plenty that you can do without writing a line of code, although of course, if you are a developer then you can do much more. You can explore all the resources on the Wix code site to learn more about web development wherever you are in your developer career. You can discover video tutorials, articles, code snippets, API references and a lively forum where you can get advanced tips from Wix code experts.

Check it out for yourself at wix.com/sed. That’s wix.com/sed. You can get 10% off your premium plan while developing a website quickly for the web. To get that 10% off the premium plan and support Software Engineering Daily, go to wix.com/sed and see what you could do with Wix code today.

[END]