uberknowledge

Yuriy Bulygin, CEO and co-founder, Eclypsium

Security in Hardware

Yuriy talks security in firmware and hardware, building a product people need, and the secret to entrepreneurial success.

02:04 How disaster can shape a career, a person.

06:24 Some hardware and firmware manufacturers are starting to pay much more attention to vulnerabilities and securing their products, but too many just don't care.

11:12 Get repeatable processes in place to scale your product, your sales, but also your team and your culture, and make it successful.

11:58 Build a product people actually need. Serve a need, don't just put more tech out there.

15:50 Security capabilities need to be properly configured - otherwise they can't protect us. This is part of the basic hygiene we should be practicing as an industry.

Ashwin Krishnan: [00:00:39] So we are at Black Hat. The last podcast conversation of the day for me, and with me I have the pleasure of Yuriy Bulygin, who is the CEO of a company called Eclypsium.

Yuriy Bulygin: [00:00:50] Yes.

Ashwin Krishnan: [00:00:50] Why don't you introduce yourself for our listeners and then we'll get into the conversation.

Yuriy Bulygin: [00:00:54] Thank you, Ashwin. It's a pleasure to be here. Thanks for having me. My name is Yuriy, I'm co-founder of a company called Eclypsium. What we do is we protect from risks and threats that target firmware, hardware, supply chain, and pretty much all the critical assets, critical devices that any organization may have from laptops to servers to network devices to storage devices, and all the other different types of devices.

Ashwin Krishnan: [00:01:31] For the purpose of our listeners, I just want to chronicle your journey. Bloomberg refers to you as "Intel's former threat guru," that's a good tagline to have your name. [Laughs] You've definitely done the tour of the name-brand companies: you've been at Kaspersky, McAfee, and the CHIPSEC project?

Yuriy Bulygin: [00:01:53] Yeah.

Ashwin Krishnan: [00:01:54] Talk a little bit about how the journey got to where it got to, particularly right now with ChipSEC, what's the motivation?

Yuriy Bulygin: [00:02:04] All right. Where do I start? Well, let me start when I was almost seven years old, I was living in a town called Pripyat, which was about two miles away from Chernobyl power plant.

Ashwin Krishnan: [00:02:20] Wow!

Yuriy Bulygin: [00:02:21] When it blew up ...

Ashwin Krishnan: [00:02:22] You were actually there?

Yuriy Bulygin: [00:02:23] I was there with my mom, and yes, I saw that happening. From that point, I got interested in things; how things work, but most importantly, how things fail. I think that defined a lot of my prior career. I focused a lot on the security and specifically finding vulnerabilities. And this is where I spent over a decade, including being part of Intel Corporation, finding vulnerabilities in all sorts of technologies from hardware to software to firmware. So, this is what I like doing. Eventually we started finding vulnerabilities, a lot more vulnerabilities, in the actual devices, in the hardware and firmware across the industry, in the fundamental technologies — the technologies that all security relies on.

[00:03:31] And we developed that open-source project called CHIPSEC specifically to enable researchers. The research community, they started poking around hardware, started poking around firmware, started looking into how those devices operate, what they are, and which vulnerabilities they have, and found vulnerabilities, new vulnerabilities, classes of attacks. That proved very useful to the manufacturers of those devices, because now they could use that project and validate their systems for vulnerabilities, for proper configuration, even before they ship. And so, I started Ecylpsium with my co-founder, Alex, to focus on that full time and to focus on the

threats targeting the firmware supply chain for our customers.

Ashwin Krishnan: [00:04:29] Very interesting. It can't get any more personal than this. Especially at the age of seven, I can't believe what kind of impression that had on your mental state.

Yuriy Bulygin: [00:04:39] I barely remember anything.

Ashwin Krishnan: [00:04:42] But it's definitely had an impact.

Yuriy Bulygin: [00:04:43] It did. It had an impact on everyone who was there.

Ashwin Krishnan: [00:04:49] Well, that's true. But I think the way you describe it, where at that point, you're driven to solving a problem that matters.

Yuriy Bulygin: [00:04:59] Yes.

Ashwin Krishnan: [00:05:00] Which is very unique. So, a little bit on your Intel background, particularly probably the biggest vulnerability ever disclosed in the history of Intel: Spectre and Meltdown. So, not so much the technical aspects, which we can definitely get into, but really as a corporation, what it did not do, despite knowing the impact. And just chronicling the days that happened after it was real — initially downplaying it, saying it only affects a very small number of people and then slowly the thing developed into something much bigger.

[00:05:40] So my question is, especially when it comes to what you are dealing with, which is at the firmware level, at the BIOS level, at the chip level, and given it's something as fundamental as Intel, but then fast forwarding that to IoT devices where it's no longer the scale of PCs and servers, it's ten hundred million times more — are you seeing manufacturers understand what it means if the vulnerability is disclosed and what the right ethical action needs to be, versus clamp down until we learn more, clampdown until we've got lawyers and have enough risk insurance in place? Just talk a little bit about that.

"There are plenty of manufacturers who don't care. They still don't have product security teams."

Yuriy Bulygin: [00:06:24] Absolutely. I think we're seeing that the hardware manufacturers and the manufacturing community and companies like Intel, they are really starting to pay a lot of attention to that, and they have been doing that for a number of years. Vulnerabilities exist, vulnerabilities like speculative execution, vulnerabilities in CPUs is very complex research. It takes years for researchers, for the research community to build that body of knowledge to start discovering those new classes of exploitation techniques. We're seeing that manufacturers, at least some of them, are taking vulnerabilities in the hardware and firmware very seriously.

[00:07:21] I believe Intel is part of that. They have a lot of initiatives internally and externally to improve the vulnerability analysis of their internal products, but also work with ecosystems to enable security features and capabilities on Intel devices. Manufacturers like Dell, they put a lot of effort into securing their devices as well. However, there are plenty of manufacturers who don't care. They still don't have product security teams. They still don't have incident response teams. There are still

outages of support at manufacturer.com or something like that. They don't know how to handle that process and they don't respond to researchers. Our team deals with a lot of vulnerabilities and finds a lot of vulnerabilities in different manufacturers, and we see companies, vendors on both sides of the spectrum.

Ashwin Krishnan: [00:08:27] That's actually good to know, the fact that there is positive movement, especially the bigger name ones. So, talking about the ones that don't have the reach or the deep pockets or even the ethical mindset that, let's say, Intel and Dell have, going back to IoT, it's assuming it's single digit or sometimes negative margins, and they don't have the security mindset. And yet, the implications of putting this in nuclear power reactors or putting this inside Horizon or deep-sea mining or even power utilities, how do you come to terms with the fact that on the one hand, it's all about a volumes game, and on the other hand, the implications of a security vulnerability that's disclosed could actually wreak havoc, at a scale that hasn't been seen.

Yuriy Bulygin: [00:09:23] Yeah, absolutely. Every vendor that builds equipment, that builds hardware or builds software, they need to have an internal product security effort, they need to have personnel or they need to outsource that function, but they do need to look for vulnerabilities in their products. If that software or that equipment goes to critical systems that we all rely on, then there is a lot more attention they should put on that.

"Every vendor that builds equipment, that builds hardware or builds software, they need to have an internal product security effort."

Ashwin Krishnan: [00:10:09] So, going back to something that I believe you posted, which is a two-year milestone that Eclypsium hit.

[00:10:18] Yes.

[00:10:19] And the thing I wanted to call your attention to is what you said was a good blueprint for budding entrepreneurs. And I quote you, "From refining the idea, to building the first engineering team, developing the product, rolling out the first customer deployments, and then scaling the team," and the last one, which I love, "building repeatable processes." So obviously, you've gone through the school of hard knocks to come up. Tell me about, not just at Eclypsium with some of the challenges you faced early on and how you adjusted, but in general, where do you see startups making illogical choices or not realizing that they have to ... is it more of the late adoption of sales people? Is it getting caught with a problem that is no longer a problem?

Yuriy Bulygin: [00:11:12] It's a very good question. It's a very complex question. So, let me try to answer at least parts of it. You know, the early teams that build technology, build products, and build business as a startup, they face a lot of challenges. And all of those challenges can be overcome, especially when those companies have help from their advisors and mentors and they look at their peers, how they've approached the market. Challenges from building the team and the culture of the team; it's very important to build a good culture of the team early on, until you can steer that into a proper direction.

[00:11:58] Building technology, of course, it's important you're building your IP portfolio, you're building, hopefully, as a new technology startup, you're building something that doesn't exist or something that is better than what exists today. But more importantly, you're not just building technology, you're building a product. And the product, backed by this technology, needs to solve problems that your customers really have. It's not something that you think they have a need, but really what they need. And so understanding customer needs, this is very key in building proper products so that you don't drink your Kool Aid but really build a product that customers need.

[00:12:53] And at some point in that process, hopefully as a company, you're finding what's called product market fit, and you start serving the customers in specific use cases for specific needs with your products in a repeatable way. And everything you build in the company, at some point, needs to be repeatable, because if it's not, then it doesn't scale and it can break. If anything goes wrong, the process can break. And it applies not just to the product market fit, to finding customers, to your sales, but it applies to everything else. It applies to building culture, to hiring employees, to building product, building technology, engineering processes. If you haven't built CI/CD systems early on, then at some point, your product will have so many buttons they will start failing customers.

"Everything you build in the company, at some point, needs to be repeatable. If it's not, then it doesn't scale."

Ashwin Krishnan: [00:13:54] That's a great point because I think — at least from what I've seen and basically what you're saying as well — that last piece of truly getting the repeatable processes in place, so you're actually able to scale engineering, able to scale sales, and get customer personas that actually fit, mean you're not building a one-off for every customer.

Yuriy Bulygin: [00:14:14] Absolutely. And as a CEO, I hope I'm learning, and I am learning with the company. This is what makes it so exciting because prior to founding Eclypsium, I had zero, absolutely zero knowledge about how to run the company and how to grow the company. The fact that the company grows, allows me to grow with it, hopefully. That's my suggestion, to grow with your company.

Ashwin Krishnan: [00:14:41] Great, that's actually a great piece of advice.

[00:14:44] So, going back to a tweet that you recently commented on from Phil Venables. He talks about "Many well-known security incidents appear to have a common pattern. They're not the result of some awesome attacker capability to exploit some hitherto unknown vulnerability or to realize a risk from some combination of controls weakness not contemplated. Rather, a remarkably common pattern is that the control or controls that would have stopped the attack (or otherwise detected/contained it) were thought to be present and operational but for some reason were actually not — just when they were most needed."

Yuriy Bulygin: [00:15:16] Yeah, I think I remember that. I was trying to see if ...

Ashwin Krishnan: [00:15:20] I was going to walk you through it, and I was looking at

your face to see if you remembered. So, it's actually interesting, but I had to read it a few times to realize that. Why is it that we miss the common ones? Are we bounty hunters seeking the most, I don't know, sexy-looking attacks? Versus maybe it was misconfiguration here or maybe an unpatched piece of software over there. So, talk a little bit about that as a security industry.

Yuriy Bulygin: [00:15:50] Yeah. I would like to kind of bring the answer to the firmware-hardware space because this point applies to everything. Let's say you have a modern laptop and it has capabilities built into that laptop, security capabilities: secure boot, full-disk encryption or disk encryption inside the hard drive. But if it's not properly configured, and it's a very often case, there are many systems that just don't have those enabled, even though it is there and supported. It mitigates class of attacks or exploits, it's just not enabled, or it's enabled but it's misconfigured, or it has vulnerabilities and it's not hashed, those vulnerabilities were not hashed. This is part of the basic hygiene that we need to do as part of the industry and across the entire stack from the software, from the top-layer cloud configuration and the software applications but then OS patching, hypervisor patching, all the way down to firmware and hardware. Same exact problem. I think this is a significant gap and significant cause for a lot of breaches.

"This is part of the basic hygiene that we need to do as part of the industry and across the entire stack."

Ashwin Krishnan: [00:17:21] So is part of it also, we're at the end of Black Hat and DefCon is starting and you're out searching for the next big thing. As security researchers or even a security ops person, telling people what you do, "Oh, I spend half of my day patching unpatched systems," that doesn't give you any kudos in the community, doesn't help your resume. So is there a personal angle to this also, where going after a blockchain attack or going after some kind of adversarial machine learning gives you the adrenaline flow versus, like you're saying, the basics are left unpatched.

Yuriy Bulygin: [00:17:59] I think both are important. We do need to find vulnerabilities in new technologies that are being adopted and new types of classes of exploits, absolutely. But we also need to take care of the basics.

Ashwin Krishnan: [00:18:14] So, last question: what does Black Hat mean for you? Why are you here in the first place?

Yuriy Bulygin: [00:18:22] I've attended Black Hats for a number of years over a decade, both Black Hat and DefCon. I spoke at Black Hat. I was fortunate enough to speak at Black Hat a few times. And usually, it's a very high-quality content in talks that I have observed over the last decade. My personal opinion is that it stays at a very high-quality level up until today, and I'm hoping that will continue.

[00:18:59] At this point with Eclypsium, it is also a great opportunity for me to spread the word about the company and the problem we're solving for our customers and also just network with fellow researchers or fellow companies.

Ashwin Krishnan: [00:19:22] Excellent. I wish you all the best and this has been a great

conversation. And you're the first guest that I've spoken to on topics like hardware and BIOS, which I think is often missed when we talk about things like cloud and IoT.

Yuriy Bulygin: [00:19:41] It is the biggest gap. Absolutely. Thank you, Ashwin.

Ashwin Krishnan: [00:19:43] Great chatting with you and good luck in the future.

Yuriy Bulygin: [00:19:46] Thank you. Thanks for having me.