Heather (00:03):

Welcome to the Hurricane Labs Podcast. I'm Heather, and today we're going to be talking about security and the internet of things, the ever increasing number of connected devices in our homes, workplaces, and communities. So today I have several members of the Hurricane Labs team here to talk about IoT from the InfoSec perspective and the challenges and opportunities these devices offer. Thanks for joining me today, everyone. Why don't you go ahead and introduce yourselves.

Josh (00:42):

Yeah. My name is Josh Silvestro. I am the lead SOC architect.

Tom (00:48):

My name is Tom Kopchak. I touch Splunk and everything else that people ask me to do here.

Kurt (00:54):

I'm Kurt. I work in the SOC department as a security architect.

Austin (00:59):

I'm Austin. I'm a part of the T1 SOC team.

Aaron (01:02):

And I'm I'm Aaron. I'm one of the T1 team leads.

Heather (01:08):

So now IoT refers to all of the devices like Alexa, and my wifi connected, slow cooker, and smart TVs, but we also see them in businesses where they fulfill roles like door access and medical devices, like heart rate trackers, and or even like customer metrics track a metric tracking. So these are really, really quite prevalent. What sort of challenges do these tools–do these devices present?

Tom (01:42):

I'm very disturbed by a wifi connected stove.

Heather (01:45):

Oh, it's fantastic. Because like, I'll put I'll thaw out the meat overnight inside the slow cooker. And then if I forget to start it in the morning, I can just start it from my phone when I'm at work. Obviously it's not an issue right now, but it was very useful when I was leaving home at some point in my life.

Tom (02:03):

It's also good to know that anyone else in the internet can turn.

Heather (02:06):

Yes. Yeah. That's really exciting. I'm really actually excited for when Alexa can actually put the meat into the slow cooker and then start it for me. But we haven't gotten there yet.

Tom (02:16):

At that point, just make her go to the store and buy everything too.

Heather (02:20):

I already do all my shopping online and have them deliver it to my house. However, it would be really great if she could like, just get it off my front porch and bring it in.

Tom (02:28):

Well, they're talking at Splunk .conf a couple of years ago, how like an airport in Dubai, they have all kinds of monitoring in their bathrooms to figure out like if the soap level is too low and that kind of stuff. And also keeping track of like, what percentage of people washed their hands and stuff like that.

Aaron (02:45):

It sounds like the same kind of thing.

Tom (02:48):

Yeah.

Aaron (02:48):

The other one that I had from later on was actually Starbucks utilizing a lot of IoT stuff to mine data from their consumers so that they can kind of like figure out what certain people like, so they know what other things to recommend people that buy that same stuff. And then it also lets them kind of remotely update recipes and stuff at specific locations that, you know, might cater to a certain kind of customers. I dunno. It seems like they're using a lot of data from these IoT type devices to help–.

Kurt (03:21):

Sales.

Aaron (03:22):

Yeah, exactly.

Kurt (03:24):

It's almost all sales. What do you think Alexa in your house is doing?

Heather (03:26):

Right. So what sort of issues do these devices present?

Aaron (03:32):

I guess one of the first things that comes up is just the enormous amount of these products that are out there and which ones to trust. The end user is left to kind of researching all of these things and the things you end up buying are usually either the cheapest or the biggest names. And when you go with the cheapest, you're obviously going to have a lot more security concerns with those kinds of things, because they're less updated, less maintained. So some users might not be thinking about that. They just want to get this product that does this thing and not realize that they might, you know, become part

of some kind of a compromised network and not even realize it. So that's probably one of the first concerns that comes to mind.

Kurt (04:17):

Aaron. And another thing to throw that too. I mean, if you could like off the top of your head, even guess how many people even think about that when they're buying any of these devices? Like, oh, this one's probably, you know, reaching out to China. Like, I don't think like, unless you really work in a security field or even in it at all, like, do you really think those, those ideas crossing anyone's mind in the first place?

Aaron (04:39):

Yeah, for sure. Most of the time, I would say it's, it's unlikely. Most people are just trying to get a product that does a thing they want, you know, they're pretty lights to come on when they walk in the door or turn them on, you know, they're not thinking about these kinds of security concerns. It's buy it, plug it in, connect it to the internet and go. But yeah.

Josh (05:01):

Well, and I think that that comes from trying to be secure by design, right. You know, really good products are secure by design or unfortunately, practice that have gone through some bad stuff–some hacks or incidents, or really big publicity, now try to be secure by design. You know, in pretty much any industry to some extent has always had something like that, right? Like when people were buying cars 20 years ago, they didn't care about the security system in the car or all these auto braking and features and things that we've just come to expect now.

Tom (05:28):

20 years ago, they barely cared about airbags and seat belts though. So.

Josh (05:32):

But that's true, right? Like, because when you're buying a product to turn your lights on, you're wanting to turn your lights on. When you're buying a car, you're thinking about potentially a luxury item to get you from A to B, you're not thinking about the things you need to stay safe, right? Like a seatbelt the airbags, auto braking, stuff like that. And the same goes for IoT devices. You know, people are looking to turn on their lights or start their slow cooker. They're not thinking about how secure that process is.

Kurt (05:56):

They're buying for the need that they're strictly looking for the want and the need of buying the device. And not really looking outside of that.

Josh (06:04):

At least in line with you know challenges in IoT. It kind of goes with challenges in the workplace with IoT. One of the things that makes IoT especially difficult within the workplace is that they're so easy to set up most things nowadays, you just plug in, it grabs its information. Sometimes you have to download an app to do something, but, but even then the process is so simple, you know, compared to, if you were trying to hook a computer to the network, all the setup and stuff you might have to do. So if you're a business and your network isn't extremely strict and in tons of policies in place that are kind of

constantly being updated and monitored, you know, in theory, someone could walk into your office and, you know, plug in an IoT slow cooker or Amazon Alexa or whatever, have it connected to the network because it's convenient for them. Or they find the functionality at work to be, to be great. Meanwhile, you know, that kind of leaves your network open for attack.

Tom (06:52):

It's not unlike the whole situation with channel IT in the cloud, even just kind of a different avenue, but it's the same fundamental thing where if someone wants to do something, they'll find a way to do it.

Josh (07:04):

Yeah. And I mean, and I think that most people might not think like, oh, you know, at our company, we don't do that or you don't see that. But unfortunately we hear plenty of stories here in recently I heard that one of their satellite office, which they thought was rather secured, they didn't realize for office management to make life easier, went around in place to replace every single thermostat with a smart thermostat, which caused some compliance issues and some other things. But no one was aware until there happened to be an onsite visit. So, I mean, it's something that just becomes normal for so many people in home life that if you're an office manager, well, it'd be grateful to adjust the temperature on the weekends when we're not there or, or check in or be nice for the lock, the doors, make sure everything's locked up and secured at night. So, you know, if you're an office manager or an employee or whatever the case may be trying to make everyone's life easier. It's, it's not a, it's like a no brainer to swap out the locks for smart locks, thermostats for smart thermostats you know, lights for smart lights, not realizing that every single one of those things you plug into the network is not only now part of your network, but also potential breach point. You know, if something down the road happens, you know, you don't want to be in the news because your network got hacked through a light bulb, but as everyone knows, the infamous fish tank story in, in Vegas, you know, anything's possible.

Kurt (08:16):

So let's say I was a manager to a larger company and I wasn't really, you no, tech savvy at all. What do you think would be like the best way for me to go about setting up some of the devices? Like what would be some procedures we would take into consideration for me to put in the smart lights or even set up blocks the right way?

Josh (08:35):

Yeah. Sure. I mean, whether it's at home in your personal life or obviously, especially in a workplace, you know, you should have a segregated network set up all your smart light bulbs, smart locks. Alexa's anything that connects to the network that is an IoT device should be on its own network. That way, like worst case scenario, you know, your light bulb has some kind of vulnerability in it, or your thermostat gets hacked. You know, it really limits the potential for a hacker to kind of pivot throughout your network from those initial entries. I mean, if anything, they'd be limited to pivoting between other devices in your network, I'm sorry, like IoT devices, you know, their light bulbs or whatever the case may be, which still could have its own hazards rate of someone cranks up all of the thermostats and tries to overheat the building and cause issues. But you know, the first step is having them on their own network to just limit their exposure to everything else.

Kurt (09:25):

Yeah. So you're essentially saying go set V-LAN and then have maybe like one management device that you could access to IoT, you know, everything from there and keep it away from touching any of your critical servers or anything of that, that standpoint.

Josh (09:39):

Yeah, definitely. You know, the truth is, especially if you get into the realm of smart light bulbs, which I know a client was talking about, they started doing that for energy efficiency. I mean, that's, if you think about a building and think about all the lights and then in a very small office, let's say you have got 40, 50, a hundred light bulbs, and those are all IoT light bulbs. That's essentially like having a hundred little computers on your network that someone could try to hack and get into your network.

Kurt (10:02):

Yeah. And just to you, funny, you bring up, I have very few like kind of odds off things in my house that are connected to the internet, but I do have some Philips hue, light bulbs, and I'm not sure if you've ever taken the time to go through and run a random app against it, or even do a TCP dump. But I actually look at what's going on, but the amount of ports and services that are opened up just from plugging in the light bulb and setting up the Hugh bridge is atrocious.

Tom (10:30):

So I was doing something similar on like a smart light switch running Nmap against it. There weren't actually as many ports available, but there's like APIs that you could get a lot of information disclosure out of. And it potentially even remotely control the thing on the same network using Python. So that was kind of interesting. Basically assume that, you know, someone on your network can do whatever those devices can do remotely.

Kurt (10:55):

I mean, here's another thing to even think of too, like the average house and everything. Like, even if you have a game system, I know for the, for example, Xboxes, or even on a PAC and stuff, like you have to set up port forwarding to get anything, to even work with your games or what not. I mean, and then 90% of the time is you got to look up like some kind of, you know, example online on how to set up port forwarding. It basically is opening your entire network up to that port, not just, you know, to a dedicated device. And if you did something to that extent, and let's say your Hue light was running at the end of the port, you just forwarded out to the internet. I mean, what Tom just said, you could probably run APIs against that just directly from the WAN address.

Tom (11:36):

And the other thing, it's not like your IoT devices typically come up with a manual that lists all of the services they need in the act two and all of that. I mean, commercial products that like they don't active directory, doesn't tell you that either. So.

Kurt (11:52):

We use an AD could probably end up doing it. The thing is with any of the, like Josh said back to the how simplistic it is sometimes to turn this stuff on. Like sometimes it being over simplistic makes it hard to actually fine tune it for security purposes because you don't have the ability to turn off, you know, I

don't want it sending, you know, feedback back to Hue or whatever for Phillips Hue lights or whatever. Like I maybe don't want the data getting sent back. I don't have the option to turn it off.

Tom (12:20):

Yeah. And it's probably in the vendor's best interest, at least from their perspective to not let people do that too.

Kurt (12:25):

Exactly.

Aaron (12:28):

The other downside too, is if you're not doing anything special on your network, so you just have like an ISP router, you don't even have that option too. Even if you wanted to do a V-LAN or firewall it off.

Kurt (12:40):

Yeah. I forget everyone here is running mostly like pFsense or some kind of open source firewall. I mean, I mean, consumer products, like you just said, Austin don't even really give you the choices to do that.

Austin (12:53):

Right. And in that situation, like if you're just running a consumer router, I really, the only thing that you can do is maintain best passwords. And then, you know, at that point you're assuming risk by plugging in that device. And it's just a matter, it comes down to how much risk you want to put onto yourself. You know, if, if your light bulb, for example, your Hue bridge gets, it gets popped, or if your front door lock has a vulnerability and now everyone on the internet can, you know, send a command or you know, to open up your front door. That's, that's a risk that you have to take.

Tom (13:32):

And I think one of the things to consider for that is, yeah, there's your local network security side of things and sure, there's port forwarding and stuff, but I think it's fairly unlikely that the average consumer is going to actually have, you know, IP addresses publicly forward into their IoT devices. But you're putting a lot of trust in the vendor to secure their infrastructure or their cloud infrastructure that's keeping that all running. And as we know, vendors have a strong history of having very secure cloud platforms without things like S3 buckets and databases open up to the world. So we don't have to worry about that at all. Sarcasm.

Kurt (14:07):

Don't forget those default passwords time that are hard to change.

Tom (14:11):

Oh, you mean like one, two, three, four, five, six, or whatever they like to use.

Austin (14:16):

And that's the bad part of it is like, there's not, there's not in place standards to enforce vendors for having secure passwords or like whenever something happens, you know, something hits the news that

a vendor has gotten you know, popped at that point. I mean, for the most part, they can't go back and change all those default passwords. So any new device going forwards may have a change password or have the ability to change the default password, but any device that's older you know, it's still vulnerable to that.

Tom (14:50):

So I think that California actually passed a law a year or two back banning default passwords in consumer electronics. I don't remember a lot of details about that, but that's an interesting thing, at least providing a mechanism to make it a little bit harder so that there's not that low hanging fruit element of stuff.

Heather (15:10):

Would those standards be something like Biden's a cybersecurity executive order?

Josh (15:16):

I know a little bit about it, but some of that ties in I mean really at a whole Biden's trying to push forward standards and things like we have for other utilities and whatnot in the United States trying to push towards standards that we have to follow for security primarily focused at businesses first and vendors. If my understanding of is correct. So that way there is some level of accountability.

Kurt (15:40):

I mean, what Tom was saying. I mean, as far as California has some wonky stuff they do, but that would be a, that'd be a law that I would be all for. Cause it really would prevent a lot of mistakes.

Tom (15:52):

Yeah. That the chemicals in this product will cause you to die. Also, there's no default password.

Kurt (15:57):

Yeah. That's fine. I'm cool with that clause. But, so we've just listed all the, you know, a lot of negatives of having IoC devices, but do you feel like there's, what are the pros of having them? Do they outweigh the cons of the potential of opening up your network to two attacks?

Tom (16:16):

Kurt? Did you just call them IOC devices?

Kurt (16:18):

Yeah, I did.

Tom (16:19):

That's amazing. If you have IOT, you have IOCs.

Kurt (16:23):

It's all the same stuff.

Josh (16:27):

There's tons of benefit. It just, it just like everything else, you know, how does that weigh for you? You know, personally in my house, there's very few things that aren't connected to the internet and a lot of people are like, oh, well your in security, that doesn't make sense. I'm like, yeah. But like I understand the risk. It is on a segregated network. I mean, I accept the information that I'm sharing. I mean, I accept the things that Alexa can hear and, and that's okay. That doesn't bother me, but you know, the, the peace of mind they have you know, we have a dog at home, so if I'm out and there's a fire, like I'll get an alert right away. You know, in the, in the early spring or late fall, when there's those weird days where it's generally cool all around, but suddenly, you know, jumps to 90 degrees, I'll get an alert saying, 'Hey, you're upstairs where the dog normally is is getting really warm.' So I'll turn on the thermostat remotely. And like that gives a lot of peace and comfort or we had a pipe break last year and we had some contractors in and out while we were out of town. I didn't have to give them a key or anything. They just let me know when they got here, I was able to unlock the door. And heck even last or two weekends ago, I wasn't home. And UPS showed up ring the ring doorbell. They said, well, we can't leave this roundabout, leave this outside. So I opened my garage remotely. He slid it in there. I saw on the camera, walked out and I closed the garage. Like for me, those things make it way worth them. But again, I understand the risk and the trade-off for me is okay. One of the first things I put in was a ring doorbell and the IDS picked up a clear trap or a clear text authentication way across the network, which I thought was really crazy. I was able to grab a packet. I looked at it and sure enough, anytime I viewed the camera or do push the doorbell in order to connect to the cloud service, it was actually plain text sharing my email and password to connect, which luckily, you know, I've got a unique password for everything. So truthfully I didn't care again. But then it was just like, I did send something into, into Ring, but it was like two months later is when they came out and said, 'Hey, here's a major update for clear text that was brought to our attention by whatever security research team they use.' So I think it's important kind of touching back on like security. Not only is segregating networks important, but I mean, you should still be monitoring those networks. If you're a corporate entity and you have an IoT network and everything is segregated, you should still monitor those things. I wouldn't just consider it, you know, walled off and safe and secure or who cares, what happens over there. It's still good to know. And things like that, you know, IDS on that network or some basic monitoring, looking for devices, trying to connect to each other.

Kurt (18:59):

I totally agree. Just, just cause you isolated, the IOC devices doesn't mean, you know, you still can't pivot around in the same V-LAN and you set up still doesn't mean it can't call out to the internet. It still doesn't mean you can't control things. You still want to know what's going on. You're just really the only thing that V-LANS are doing is preventing it from maybe hitting, you know, your other computers on your network or, you know, if you're in a corporate environment, many or servers, et cetera, if you don't go about setting that up the right way, if you didn't know that that was sent over clear text, like say for your password and you didn't recognize it and you didn't have your password, you know, individual for each one, like for example I know a lot of my friends use like, you know, the same password for everything or, you know, don't ever even use anything over eight, eight characters that, that could have caused stuffed on their end to get compromised on it without having the knowledge to do all the other security practices on it.

Josh (19:51):

Yeah, definitely. You know, and that's the hard thing. Again, products are all designed for what they're to do first and insecurity is definitely an afterthought. And just to kind of cycle through different vendors, you know, you're talking about Ring you know, a couple of years ago, a friend of mine had some troubles with the Nintendo switch he got getting out to the internet and it was like a very unique issue. So I was looking through Nintendo support articles and one of the things they recommend and they said sometimes ISP-provided routers can cause issues. So we recommend removing the router and connecting your switch directly to the modem, to play games. And I'm like, you know, that's, that's a big no-no for anyone in security. You're like your first thought is, you know, not even a basic router between you, you're just putting your switch on the, you know, the internet for anyone to use.

Kurt (20:36):

Yeah.

Josh (20:36):

But that's cause at the end of the day, Nintendo doesn't care about the security. They want, you be able to play your game. So you keep buying games, you keep using their service and that's true of any product, right? If you're Samsung with smart things or apple with their home stuff, like the truth is the thing you care about is people buying more of those light bulbs, more of those thermostats or more of whatever. And if you're one of those companies, that's lucky enough to stay on the news for security thing, then you don't ever really care.

Austin (21:01):

That's a, that's the nice thing is you, as a consumer can essentially pick and choose what products you want on your network. I mean, there's different protocols instead of going wifi to have all your devices connected. If you're a little bit more technically savvy, you can use something like Zigbee, which is uses local, a local radio frequency to turn on and off switches. Then you would use like a service such as like say home assistant to pull it all together. I mean, the guys here know how much I, I personally like home assistant but it, what it is, it's basically a open source web server slash platform that you can feed all the API keys for your IoT devicesand have one panel. So you can build automations. And I mean, I can go down that rabbit hole for a couple hours, but basically if you don't want to have a device that's cloud connected, there, there are options. For example, just a website off the top of my head cloudfree.shop, they sell nothing but devices that are flashed to work over the land. Only it doesn't reach out to any sort of cloud service. You can scroll, you can still access it. I mean, if you want to access it outside of your network, of course you'll have to port forward home assistant and do all that fun stuff, but you have the option to choose the devices that you want on your network.

Kurt (22:22):

So I guess one of my next question was, is, I mean, what you said, Austin, I mean, all that's awesome, but I don't think the average person, I mean, hell is setting up the radio frequency and trying to do that to control some of the stuff around my house would probably be a task for me to figure out from the start, but–

Austin (22:38):

Right. That's definitely like an advanced level. But like if you were interested in setting up something like home assistant, even they, they make like image installs now that you can throw on a raspberry pi or they even have a standalone device, it comes flash with homesis and all you do is plug it in and configure

it. I get that what we were talking about earlier, how easy it is to set something up doesn't necessarily mean that it's secure. But the nice thing about homesis and being open source is that it's one of the bigger projects on GitHub currently. And there are constant push requests to a daily. So you can actually go back through and do code review to determine if you're safe or not. And it doesn't, that comes down to risk. How much risk you want to actually put onto your network, how much you want to assume.

Kurt (23:22):

What would you say are some good ways since we've talked about all the like crazy technical stuff that we could do to, you know, set up V-LANS or things that are kind of out of reach of the normal consumer, what do you guys think are like some good recommendations that the average user could do to try to keep their stuff secure?

Josh (23:39):

I guess, you know, even before trying to secure network and do all that pickup brand you trust and like Apple has a good history of being secure. Yes, Samsung, depending on the product has a good history being secure, but–

Austin (23:51):

Yeah, that's also, that can also hurt you too, too, because you'll get put into, you know, the Samsung ecosystem with smart things and, or going down the HomeKit route with Apple. I mean, it, it, it does come down to a brand that you can trust. I mean, that's, that's one of the other benefits that I personally like about, you can pull those different brands together and have one ecosystem, but if you're going to stick with just totally one, one brand, definitely pick someone that you can trust.

Aaron (24:18):

I mean, outside of like sticking on brands, though, if you put, you know, outside of like relying on the third party, like even just setting up a password manager, like something that you could do, or even setting up two factor on all your log-ins on things kind of things that the end user could do without having to rely on a third party.

Josh (24:38):

Yeah. I mean, I think–So again, I don't know that you can't, at least I know there's tons of custom stuff you can do, like we were just talking about, but the truth is for, you know, as you asked the average consumer, or even what you're more than likely going to go ahead and see in a corporate environment, the kind of devices that are gonna sneak in, aren't going to be those extremely custom things. They're going to be the plug and play things that tie back Apple's home kit, or I personally have been using smart things forever. And the nice thing is, so, and I'm not talking about like brand loyalty in the sense that like, why I love my iPhone. So I'm sticking with apple, it's, you know, to choose a company that even if you like their products, that they have a good history, that they have security involved in their products. And even if, you know, Apple's had incidents, Samsung has had incidents, but they've become brands for being reputable for trying to make secure choices, but, you know, humans, aren't perfect. So codes aren't perfect. But if you pick a good brand smart things, for example, through Samsung, or even set up their product, their hub to control everything, you have to have two factor on your account. Anytime there's a sign in to a new sign, into the smart things app from a phone that hasn't seen before it lets you know, like that, that comes down to choosing a brand you trust that's, I'm sure apple does the same

thing, right? They're enforcing two factor in all of their devices, their phones. So I can only imagine their home control devices are the same.

Austin (25:52):

And even Google just announced this week that they're going to start enforcing two factor.

Josh (25:58):

Perfect. Great. And so the nice thing is you know, there's definitely a standalone and stuff you can get that are all IP based, but you make a good point when you talk about, you know, how everything connects back to the hub, right? So pretty much every light bulb and lock and everything. My house is either a ZigBee or Z-Wave and connects back to the smart things hub. The benefit of that is, you know, you don't have to worry about a hundred different devices per se, and how they're configured. You're really relying on Samsung to be doing the right thing within this hub. So it's more about managing one product in theory, controlling 20, 30, 40 other devices.

Heather (26:35):

What about on the manufacturing side, what companies who are making IoT devices can sort of watch out for what they should be watching out for that they aren't?

Josh (26:45):

If you're the manufacturer of the product, you should be trying to be secure by design, right? Using coders and people that understand security, having a proper life cycle process for software to review and make sure that the software is constantly up to date with best practices and being reviewed to find any kind of issues that might have been overlooked during the development process. And then touching on what Aaron had said, you know, making it secure by default, right? Don't when the app is opened by default, have it be as secure as possible, you know, force two factor authentication have, you know, if, as far as privacy stuff goes, have those boxes unchecked and require checks to opt in, you know, and–

Kurt (27:22):

I would love to see that some

Josh (27:24):

Products do that. Not many, but some do.

Aaron (27:26):

Yeah, I guess the only other the only other item I had regarding manufacturers is that not every place may be able to have a dedicated team of security minded individuals. And I think that that's where some places like Microsoft have tried to attack that market people who can't necessarily do the security for themselves, but will pay for some kind of a service to make sure their, their product has some kind of a we're protected by, you know, this big name kind of thing. So Microsoft's developed this Azure sphere platform, which is a chip that you can put in your embedded IoT kind of device, and then they manage security on that device for the life cycle of that device. That is an option where if someplace does not want to dedicate to having a security, like a full blown security development team.

Heather (28:14):

Alright. So what is one key takeaway that individuals or businesses should have about IoT?

Aaron (28:20):

Be smart about your password. That's my top.

Josh (28:22):

One. I would say that it's kind of inevitable. So make sure you're choosing a brand you trust, or at least a brand new trust enough to what the, how they're gonna handle your information and that they're gonna maintain their product to try to keep you, you know, your business or your home safe,

Tom (28:37):

I'm thinking, understand what the devices are doing, what connections they're making, who they're communicating with. And if you don't know what's happening, it's hard to understand and control it.

Kurt (28:46):

I'm probably the more cynical one yeah. With all of the IoT stuff. But if I were to give one takeaway with all of it is I think when you find the right product, you can definitely find IoT devices that the pros will outweigh the cons. I just think you gotta be smart with the decisions you make as far as who you're buying it from and how you're sending it up locally on your network.

Heather (29:08):

All right. Well, thank you very much for taking time to talk about this today. We appreciate it.

Kurt (29:13):

No problem.

Tom (29:14):

Thank you for having us Heather and that's all for today.

Heather (29:17):

Be sure to check out our links below we've put together a checklist detailing ways that you can better secure your devices as well as a number of other resources regarding IoT security. Until next time, stay safe.