FINISHED FILE

INTERNET GOVERNANCE FORUM USA 2021

The Road to IoT Security: Industry and Government Working Together

JULY 15, 2021

12:15 P.M. - 1:15 P.M. EASTERN

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
1 877 825 5234
+001 719 481 9835
Www.captionfirst.com

***

***

>> DUSTIN LOUP: All right, everyone. Welcome back from the break. I hope you all had a nice refreshing time to digest the last panel as we move into more security discussion. So as folks trickle back in, I will hand it over to Shane to introduce the panel.

>> SHANE TEWS: Thanks, Dustin. After that last discussion, I'm glad that I'm introducing you to a bunch of

problem solvers because that last conversation, which I had many times just always kind of freaks me out a little bit. I feel like we are not completely in control.

So this discuss has been going on for a long time. We had several times at the IGF and we have always gone back and forth with the two different levels of conversation. One is the consumer level, because there's a lot of us sitting in rooms with a lot of devices but with the advent of 5G and Next Generation networks, we are seeing a huge change of how the Internet of Things is being handled at the industrial, in the commercial, and the -- you know, more than the consumer level which is really where we will focus today.

So welcome "To the Road to IoT Security" panel. The idea of IoT security took off with the Mirai attack where service attacks were using devices to create a bot network. I realize this is a sophisticated group. And this brought forward the security issues by IoT. We have now seen the advent of Internet of Things connection. So there's an entire ecosystem that calls on the manufacturers at the very beginning, like Intel, who we'll hear from today to work with the manufacturers of the e devices both big and small to adhere to agreed to policies and principles for the security by design.

This means promoting security that interoperable, scalable, measurable and has a global application. Drafting these international standards and policy guidelines have created conversations that are both cross industry, consensus driven and approaches that have brought together governments and industry, the engineers and the lawyers, as well as created public/private partnerships that are multi-sector and allow for widespread deployment across networks for rapid growth of these really complex networks working together.

So I am going to ask each one of my panelists to talk for a couple of minutes about their part of this ecosystem and then I look forward to a healthy discussion. Paul, I will start with you. And Paul Eisler is with USTelecom, he serves as the

Secretariat of the council to secure the digital economy, which is an amazing read. They have done an amazing job of getting a lot of this complicated stuff in a succinct document. Paul, tell us what you have been working on there and how this is important to your constituents at USTelecom.

>> PAUL EISLER: Thanks, Shane.

So if you spend enough time in Washington policy circles, you heard term "public/private partnership" thrown around a lot. I hope this panel shows that tremendous progress is made towards securing the Internet of Things but also that the collaboration, the genuine partnership between the industry and the government is a model that can be exported because it works, and we can use it for future success.

To that end, when you talk about why policymakers and why industry cares so much about securing the Internet of Things, there is, of course, the attacks like the massive attack on dine that you mentioned. There's also the propagation of many different types of malware, including ransomware such as you have seen in the news a lot of incidents, surrounding ransomware.

And have you also seen the propagation of disinformation campaigns. There's this astounding study at Carnegie Mellon that found during the height of COVID-19, somewhere between 45 and 60% of Twitter accounts discussing the pandemic were actually bots and not human beings. So for many policymakers as we said, the big call to action was in 2016, when the now historic bon net attack took place on the dine. And the Council to Secure the Digital Economy was formed. The acronym we use is CSDE, and the website is CSDE.org. Mike Bergman and I were part of the Secretariat and meet on the steering committee. This is comprised of 15 global ICT leaders and comanaged by USTelecom in partnership with CTA. And the purpose of CSDE is to address problems that cannot be solved by individual companies or segments of the global ecosystem because what we need is a holistic solution, what we need is cross-sector partnership and we need everybody to cooperate and do their part.

So that's why we also have numerous partners across the ecosystem that endorse individual projects. For example, the IoT security policy principles which were published earlier this year, these were endorsed by a total of 27 and counting organizations across the United States, Japan and Europe and we're starting to engage stakeholders in Latin America as well, although conversations are still in the early stages.

With we publish an annually updated guide for fighting botnets. It was translated into Japanese. It was cited in publications of the global Internet Governance Forum.

However, when we originally published the guide, there was -- the original iteration of, it there was no technical standard for IoT. In fact, there wasn't even a published consensus baseline that industry had affirmatively said yes to at the time. We saw this as an opportunity to contribute to NIST's efforts and demonstration that the public/private partnership is more than a series of talking points. It's an operational reality.

So in parallel with NIST's development of the core baseline in IoT, CSDE brought together dozens of convening organizations, we are talking trade organizations and standards development industries, industry alliances, coalitions and what we did is we leveraged the expertise of their hundreds of technical experts and ultimately formed the seed to consensus baseline. They continued to update the document, resulting in CSDE's publication of the document that we continue to refine.

The C2 consensus. This maps NIST 82-59, and it provides common set of capabilities that can be applied across all in IoT devices and there are now important technical standards, built to translate into a language that can be implemented by engineers. We also have ANSI CTA20-28, and now that we have this guidance that's detailed enough for engineers to implement an IoT security baseline. The next step is how do we built international standard settings.

ANSI, they are ultimately an American organization and there are other standard institutes in other parts of the world. So we are now in the process of developing an international consensus, and you will hear more I'm sure from the other panelists about this, who are deep in the trenches and contributing to this important effort. We have multiple standards that have been or being developed for different industry verticals.

The high level takeaway from all of this work is that our goal is to raise expectations for security throughout the global marketplace, because cybersecurity has no borders and the best solutions will be the international ones.

>> SHANE TEWS: Thank you, Paul.

It was a great introduction. Adam, most priority thing I need you to do after I introduce you is explain what 82-59a is.

Which I'm looking at the -- and I know it's now in Portuguese and Spanish. That's most important.

So Adam Sedgewick is the senior information technology policy advisor at NIST, where he works on standards as we're hearing about right now, and he's been in a major advisory role at NIST and the related technology issues. Those are all the things I think that NIST does. As far as I'm concerned, Adam, you are in charge. So how is it going? You know, you are our government stalwart on this and what the hell is 82-59a?

>> ADAM SEDGEWICK: I promised myself I wasn't going to speak with NIST acronym and numbers, but --

>> SHANE TEWS: You have to because someone will slide into it, right?

>> ADAM SEDGEWICK: So, yeah, thanks for having me. Thanks for the opportunity to speak. Just to talk a little bit about what NIST does overall, and Shane mentioned a big part of the digital work, but we do quite a bit, and our overall focus is all around measurement, which Shane also mentioned.

And we are a national laboratory. We are actually part of the government, within the commerce department, but being a non-regulatory agency, actually has given us the freedom to collaborate with stakeholders on their same level, right? So there are discussions around voluntary versus mandatory when it comes to cybersecurity. Our role is heavily geared towards the voluntary, and we think that's very successful, because it allows us to work with the greatest number of stakeholders possible. So it's not about do I have to do this? Should I do this? We found -- we find really our strength by working with people to do things that they want to do because it benefits them.

IoT is an interesting example of the type of work we do. I think we grapple with it for a long time. We called it different things. We called it cyber physical systems. Partially because I think if you were to put a list of all the things that we do in cybersecurity and privacy on a dart board and blindfold yourself and throw that dart, would you land upon something that has to do with IoT. Our workforce and awareness work has a lot to do with IoT, because that's how people are going to be acting with the Internet and have cybersecurity and privacy considerations.

Our work in encryption will have to do with IoT because encryption has a lot of power demands. So we do a lot of work with encryption and low-power and constrained devices.

And a lot of use cases are going to be really different, right? You are going to want to have different security capabilities at the IoT device, if it's something that's helping you stay alive, versus something that's just a note in a highway that's delivering some information back to the Department of Transportation periodically about the health of the highway. It's also important. It's just you might have different security and privacy considerations.

So the role of NIST in this space, it's twofold. A lot of what we do in cybersecurity and privacy, we have this mission that goes back a long time, in developing standard settings and guidelines for federal information systems. So if you are a Department of Transportation, or you are the Morris K. Udall, you need to help you leverage commercial off-the-shelf products. So that's to get us away from a system where we tell the technology providers exactly what they need to create for our limited use case. Instead of just trying to figure out how do we leverage innovation and what technology companies are already doing, how do we harness that to help the departments and agencies meet anywhere business mission?

So it was only very recently, for example, that the Department of Defense stopped having custom-built mobile phones, right? They realized we can just leverage what these organizations are doing and make sure that they are mindful of their security and we can leverage that for our own business purposes.

And that's where, you know, 82-59A comes in, right? So those are publications to look at foundational cybersecurity activities for IoT device manufacturers. So that's an important piece of it. While there are different uses of IoT, there are some things that on the foundation, that we should begin to expect that we can see in a range of IoT devices, because we don't have that foundation, you are not going to have -- be able to build those security and privacy and security capabilities on top of them.

That's one way in which we do this work in IoT. We also have things that help enterprises think about the devices. So you have these IoT devices and your devices ideally, they are leveraging 82-59 or some of the other work we'll talk about today, but if they are not, or if you don't have that ability, how should you as an organization think about IoT? How should it impact the way that you build your enterprise security solutions? And also are this things you can do on the network?

All of that then ties into the other part of this, which is the S in NIST, standards. We have a role in coordinating international standards on behalf of the federal government.

We also participate robustly in international standards development, and a lot of work that we do given these responsibilities under FISMA for the USG then becomes that pre-standardization research, and then we can take to international standards and is this something we can work with industry to enhance? This is truly a global issue as we already heard. So national issues to IoT really doesn't make any sense. To the actual extent that we can leverage standards internationally with industry and government, it frees up our ability to focus on the things that matter.

Instead of saying you talk about IoT in this way, and we talk about it in that way, it allows us a more common. I think I'm a little over time. Thanks again, Shane, for having me.

>> SHANE TEWS: That was a very good table setting exercise for a lot of what we are going to talk about. So Dr. Amit Eliazari, I think this is your first IGF USA. This is where discussion happens. She's the director of cybersecurity policy and government affairs at Intel and a lecturer at UC Berkeley school for information master in cybersecurity program and she's a graduate of doctor of science of law, and she has a JSD from Berkeley Law. You supply chain management has been the buzz word for the entire year. As we talk about all of these things towards the end of decision-making cycle, you guys need to be backed into this way, way early in the process to make sure that you are bringing the tools to the party that people are eventually going to use to create all the security. Tell us about your role in all of this.

>> AMIT ELAZARI: Absolutely, and I'm so excited to be here with you all. Definitely looking forward for more participation in this forum.

So, you know, as you heard, this is an ecosystem issue, right? And our role is really foundational. We are enabling the security from the foundation side, from the silicon ops from the financial sector to HLS to industrial specifically within the context of IoT. And, of course, we are very much interested in supporting the security, of specifically supporting the baseline capabilities, right for IoT as we are building this foundation.

So my role specifically, I'm part of the government relationship team. I'm one of the directors, working on global cybersecurity and I focus, among other on the area of IoT. I work very closely with our engineers in our Internet of Things organizations and with our business partners to bring the goodness and enable the ecosystem.

Thousand, as we work collaboratively on addressing the security issues, of course, we need to participate with the ecosystem in many forms. Part of this is the IoT security alliance, it's standards work, it's enabling the technologies that can help advance our problems, for example, secure device onboarding for our work in FIDO alliance and the like.

Another part is the active participation in driving best practices and driving international standards and technical conversations as we are talking about today, as well as working collaboratively with our partners with policymakers and the governments of the world, as they are considering how to regulate, how to address this issue of IoT security.

Now, we know a couple of things about IoT security, and the uniqueness of that ecosystem when it comes to security policy. It's a very diverse ecosystem. Again, we are talking in this ecosystem about everything from the potentially cheap consumer IoT device, right, which is low cost, to the sophisticated system of industrial or critical infrastructure. We know that the complexities not just about the verticalization. It's also about the fact that the IoT ecosystem is the technology supply chain in multiple touchpoints. So we have everything from the cloud connected to this, to Internet Governance, to the supply chain, to operational systems, and the like. And we also know that the complexities on the rise because the attack surface itself, of course, is still evolving.

So how do we go about this, with this level of complexity? We have some important principles, right, security policy principles that are articulated, among others in this paper, of course that the CSDE, my colleague Paul here has mentioned that has this broad consensus. But a key pillar is making sure that we have interoperability, and harmonization of technical requirements around the world. Okay? So we have the backbone of technical specifications that engineers can implement that establish the foundational footprint.

So where do we and I collaborate on this? We work very closely with our engineers on distributing to NIST and distributing to NIST 259 and A2D and we do this across aboard. We collaborate with the ecosystem partners to create the FIDO alliance, secure device onboarding, but we also participate and lead in international standards, specifically I'm one of the co-editors ISO I624-2, which is the current effort to not just contribute to the work in the US and the work in Europe, but advance ISOC, which is the cybersecurity committee to promote that international consensus, of course, with global participation and expertise, so we will have that foundation of what are we talking about when we are saying, you know, these are foundational IoT security capabilities. Unique authentication. Security update and the like. What are the details both in terms of device requirements and the process requirements. Again, I'm one of the coeditors leading this work and I'm very excited to, you know, be participating in that with the partners -- with our partners, especially our partners here on the line.

>> SHANE TEWS: Thank you so much and we really appreciate you participating with us today. Our last panelist and definitely not least, because he's the guy who helps all the things in the boxes get out to everybody who wants them. Is Mike Bergman who is the vice president for technology and standards at the Consumer Technology Association. Where he leads the association work on cybersecurity and Internet

standards. He's been in the electronics industry for more than 30 years in memory chip design and wireless communication.

So Mike, give us the -- give us the next layer out which is the person who actually works with all the people that do the deliverables. All of these guys are helping you get there, but, you know, you do a tremendous amount of work in this space.

>> MICHAEL BERGMAN: Thank you, Shane.

Yes, so as you indicated in my brief bio, I have had a career as a working engineer and engineering manager. So I tend to look at all of this despite being involved with Amit and Paul and Adam and his team over NIST, we all work together. It may sound like we are ganging up on you all in the audience, but this is awe public/private partner and you are talking to some of the partners here.

Paul described the CSDE which is an organization working in a broad sense on best practices, guidance, things like that.

Adam described NIST which has the seminal, 82-59a, and Amit spoke about cybersecurity within industry and within technical standards to that end, and Amit is a major player on that within Intel.

So now we have got a bunch of these pieces. What I would like to do is kind of go through how it all sort of fits together and how you can think about it.

So if you think about 82-59a, it's a best practices or it's a guidance document about the minimum security capability of an IoT device. When we say minimum, we mean really, you know, guys, you have to be this tall to ride the ride. That's one of the Allen freeman's favorite sayings about SBOM.

You really need at least this much. And if we can get everyone to comply with just the minimum, that would be great, considering the more botnet rampaging still and it takes advantage of some of the gaps in just minimum level of security, people not implementing minimums.

All right. So 82-59a says, look, no minimum -- no default passwords. You have a variety of guidance in there. It tends to be more contract because NIST is aiming at the entirety of the IoT system with this document. But it's like, look, just do what we suggest in here somehow and things are going to be a lot better.

I think I speak for my other two non-NIST panelists in saying we really actually believe in that. So separately, as Paul indicated, the C2 consensus came out and it is a regional -- I'm sorry, it's an industry or a sector-specific subset of the NIST guidance. It's more specific. It doesn't leave anything out. It's just more specific to a section of the IoT which is more dominated by consumer electronics, all right? Are.

So if you think of this as a cake, the bottom layer may be 28-59a and the next is the C2 consensus, now those are both guidance and then we move into technical standards. Amit and Paul and Adam all use that, I will tell you what I think a technical standard. Is a technical standard is a document that an engineer reads and he finds words like "shall" and "must."

If you were painting a house, and the owner said I want my house painted, and you said, any color? And the owner it shall be eggshell blue. You don't do it a different way. You do what the shall word says. It's a document with enough specificity to tell the engineering exactly what they need to do to be in compliance.

The NIST guidance and the C2 guidance move in that direction, and then documents like ISO/IEC 27402 which is Amit is the coeditor for, and the ANSI 23- 88, we are throwing a lot of numbers and acronyms at you folks. But the point is they have these shall and must and quantitative requirements that the engineers can understand what to comply with.

From there, the next question is, are you doing it? Did you accomplish that goal of meeting the shall and must goals in the technical standards? And this derives now from the minimum security requirements. Did you meet the minimum security requires as in these technical standard settings? Well, then we go to conformative assessment programs. There's industry conformative assessment programs that use all the documents we just mentioned, although 27-402 is still a draft. It's not jet brought in, but it's believed that it will be a very, very important document in this context.

But the document that Europe is using which is called EN303-645, there's a document that the UK's -- that the UK government put out called Code of Practice. There's other documents like this. These conformative assessment programs, where you can go out and buy testing for your product, actually wrap up these requirements and so you can go to UL and get tested for compliance to these technical standards.

That's called conformity assessment and you get an assessment from UL when you do that. You can get a similar service from Euro Fence testing. They do have a US footprint, internet tech, CTIA has a certification program as well. It's not -- I'm not as familiar with that one. I will not try to talk too much about it, but these conformity assessment programs then check to see that the product design met the requirements.

Now, from these -- from this structure, we can talk about policy elements, right. All of this is engineering and business-to-business discussions. And, in fact, before I leave this, business-to-business includes major retailers now looking at these conformity assessment programs because think of your favorite major electronics or consumer goods retailer do they want to be on the hook for shipping product that's spied in bedrooms or whatever your nightmare scenario is with security?

Now we have a lot of discussions with the retailers, I'm with the Consumer Technology Association, about how all of that is going to work for them.

So you take all of that, and now you can start making policy decisions and there's discussion about certification and labeling and all of this. That's all policy, right now I'm staying within for the moment, the structure that's being enabled by all the work of the people on this panel, to give you the tools to make policy work, because without that structure, you don't have any target for the policy to latch on to.

That's more than enough, I think and Shane, I will hand it back to you and thank you so much.

>> SHANE TEWS: There's some relationship language. Where do you want to go to dinner tonight, honey, any place, as long as it shall be an Italian restaurant.

(Laughter)

Just get it out there so you don't have a fight in the car. Great idea.

You talked a lot about engineers and several of you have heard me talk about this nightmare meeting on my birthday a couple of years ago at the request of DHS. It was all lawyers there. And all they could talk about was who they were going to sue when something hits their system and it's not going to be my device's fault because your network, blah, blah, blah, I was horrified and I left the meeting and I said if it's up to you guys the Internet would not exist, nor would any of these things be attacked and we are the people that want to help. That's one of the reasons why I'm so enthusiastic about this panel today, is the ability for all of these players in the ecosystem to get together and then come up with a self-assessment which basically says we -- you know, we -- well, actually I would like to talk about the self-assessment and how that came about. And how that is an area, where we're talking about this and where does the self-assessment come in?

>> MICHAEL BERGMAN: Yes, I can address that. That's a great one.

So if you think about all the product that is introduced every year in connected products, it's -- it's an enormous, enormous tsunami of new products and that's -- I mean that's evaluation. That's innovation right at the leading edge.

An ecosystem to test everything is -- is maybe overkill and rather difficult to achieve in a short period of time, like 3 to 5 years’ time frame.

What we can also do, though is we can rely on self-attestation, or self-assessment. Self-assessment is I check myself. Self-attestation, I assert that I checked it and I'm asking you to trust me. Now, who would -- if I'm a manufacturer, who would trust me? It's someone who can really old my feet to the fire if I misrepresent that and that's the major retailers.

Think of the major retailer and think of a very large brand name manufacturer. If the large brand name manufacturer self-attests that all of their cameras or washing machines or whatever are in compliance with a technical standard -- we talked about the technical standards.

If that manufacturer says these are in compliance and includes that with the purchase order receipt and material, and all the stuff that moves the product into retailer and the retailer is willing to accept that, that's a strong incentive for that process to work. The manufacturer has a market incentive to make that work. And comply with that and not screw up that relationship they have with this major retailer.

This is also true in terms of any kind of contractual relationship between a big buyer and a vendor.

I will say -- I mean no shade on any category of any manufacturer. We love all of our children here at CTA, but cybersecurity does require resources and the largest players have shown that they are able to spin up the resources necessary more quickly than the smaller players. So if you look at the job, the major players are doing right now, the largest brands are doing right now, they are doing a much, much better job than five or ten years ago.

You will see still there's still hacks. Researchers still reporting things. But it's -- when you look under the hood, you see that it's a much better situation.

Anyway, self-attestation is about that kind of relationship, and it plays a part and a very large ecosystem, we are going to need third-party conformance testing and self-attestation mechanisms to be recognized and valid throughout the process, because if we simply flip a switch and say everybody has got to have a UL certification, UL will be overwhelmed, industry is going to be unable to ship product, customers are going to be unhappy. It will not work.

>> SHANE TEWS: It seems like you have found the right balance to be able to collaborate with each other, and not be too prescriptive which I'm always worried about when legislators introduce -- and there have been several pieces of legislations that I have had other panels on where we've had Congressmen Marky had a great one we wanted to do this shield and I tried to explain to the staff. Are we going to be able to scan over it? You know, every -- because there's software updates and, you know, everything is constantly updating. Any time there's a legislative vehicle, you kind go into your shalls and musts. How do we make sure that the end thing -- the idea for them was no consumer harm.

I think the balance that you have struck here is really unique because as we saw from the previous conversation, there's still a group of people who are trying to figure out how to talk to each other. And there's lots of mischief in the middle space there and you all from an IoT, you know have really figured out something that seems to be at least on the path to working. So other comments on the self-assessment?

>> AMIT ELAZARI: I would just touch upon something you just raised, which is another principle which is articulated in the CSDE consensus paper on IoT security principle. It's overarching. IoT echo system is certainly one where we see tremendous developments in technology Ute case and the complexity of the ecosystem playing, as well as, of course, the attack surface. But overarching in security policy being one of the most important principles is design neutrality. The

concept of design neutrality when it comes to policy, as a whole, in technology law, is basically this notion that as we are considering regulations or policies, we should try to accommodate terminology that is flexible enough to accommodate for both future technologies, so in the technology side, both future attack surfaces, right?

Again, what we are dealing with is also changing, right? And this is very important, and a key pillar of many documents you will see across the board. That's where the advantage of technical standards come in. Technical standards are amended. Certainly there are certain bodies that do it much faster than others. Yes, amending some technical specifications and start ads, especially at that level of international standards could take more time, because of the level of rigorous consensus, right, that you have in, for example, in ISEC documents. It's getting amended with time and expertise and that's ail little bit of what is the benefit of technical standards if you want to go into the details security requirements that's why you do it in standards as well as other policy vehicles. So I just wanted to not specifically self-attestation, Mike describes a lot of ideas. And it is a key principle of our work, when it comes to IoT security policy.

>> PAUL EISLER: I agree fully with everything that Mike said, everything that Amit said. The only thing I would also add is that, you know when people think about self-attestation, sometimes people think that there's no enforcement. If you self-attest to something, that is not true, you can get into serious trouble. Any corporate in-house counsel, they would want to make shoo that you are only certifying to things especially if you are representing a legitimate company that you are only certifying to things that are factual and I think that's often not included in these conversations.

>> SHANE TEWS: So you -- you bring up an interesting point, what about the bad actors. What if you get a bad apple in that is trying to slide in. Is there a name and shame part

of this? You know we all want to be the good guys and wear the white hat but what happens when we have the people that are not playing well.

>> PAUL EISLER: So if you are a bad actor in the ecosystem, there's a significant reluctance if not outright refusal on behalf of the more legitimate players in this space to be associated and in some cases what you will see is the government taking some interventions that take the form of policy prescriptions or outright top names and the government has taken those steps where the intelligence community felt it was necessary.

>> MICHAEL BERGMAN: We can actually drop one name. I will drop a name. Dowa Technologies if you are familiar with the Mirai botnet. You though that they had devices that were implicated in that botnet in a very large way. Reports from researchers varied. They used different techniques but apparently hundreds of thousands of product from that one company were implicated in that. And now you will find that Dowa is not on the shelf at your local retailer. This is a really, really well-known example and I'm not sharing any secrets here.

I believe they are on the entity list now at the Department of Commerce's best registry of companies where you shall not do business with them. And they may also be on the FCC's list. It's not a good idea to ignore cybersecurity and increasingly, as, you know, year after year, we are seeing that it's becoming more and more an issue for everyone in the ecosystem, these bad actors will get fleshed out pretty quickly.

>> ADAM SEDGEWICK: So, Shane, I will address that question, but I will just tweak it to make it slightly friendlier to say, what do we do with the legacy issues give than there are plenty of IoT devices out there already that might not have security capabilities built in.

I think some of the recommendations from the various groups, including us, is why we take a more holistic view. What are the things we should be doing on the network level and the organizational level, realizing that there are plenty of devices out there now, that we have to accommodate, and it's just kind of the reality.

So I think there are a lot of exciting things that are happening, that allow people to sort of assess the health of these devices as they come on the network. And it's that sort of layered approach that I think all of us promote, that will help us deal with the fact that it's not just about the devices, but how the devices are being used and how they are managed as well.

>> SHANE TEWS: And a question -- it goes more to the industrial level. When you have -- when you are just the middleman on this. So I'm thinking, Paul, about some of your membership and you see something that is a potential problem, where are you guys on the information sharing perspective of hey, we're starting to see something come online and we are thinking that this is not -- you know if you had the ability to stop something like a Mirai botnet attack, is there something that we have a capability for?

>> PAUL EISLER: So our companies are constantly monitoring the network for threats. There are advances that are happening to better predict botnet attacks. The member company, NTT coauthored a paper with NIST earlier this year, on models for predicting botnet attacks before they happen, and therefore being able to allocate resources in a way that allows to you respond better.

We see peer-to-peer command and control architectures in botnets that's a bit of a mouthful but what that means is the botnets distribute control amid control on all the networks and that makes it ease err to take it down. You have Lumen, the black Lotus labs research team, they discovered Mozi, a P2P, from a 2016 attack and also IoT reaper and all of these are known to attack insecure devices that are not built to this industry standards that we are recommending.

And Mozi has been quietly assembling an army of routers for pay load execution, and you see this is just one example of one company and the research that they are doing, to address that particular threat, and very often what you will see is a company will notice a threat, and they will be reactive to the ones that they notice on their networks first and they share that with other trusted partners in ecosystem. This is not just limited to ISPs. You see folks in the IT sector. You see Cisco has a very good research team that share threat information with our companies.

So this is a whole see could system a -- whole ecosystem approaches. If the bad guys were just using the tools and techniques that they used back in 2016, we would be on top of that. We would be in a very good position to be able to contain those threats. The problem is just as our tools get better, so do theirs.

>> AMIT ELAZARI: I also want to quickly build on Paul's point. One the things you will notice if you open up those technical specification documents in the standards being right, A259b, d, I think, both you have potentially even in the CT, of course, but also in 28-8, references to a concept called vulnerability disclosure programs. So let me explain that. In addition to the capabilities and the importance to work with the ecosystem on what we call cyberthreat information, through vehicles like ISAC and we collaborate to advance our understanding about threats, there is also an important understanding when it comes to IoT, that the complexity of the landscape and the attacks surface means we will need to always collaborate with the external researchers that are doing the research work, security researchers and able that collaboration and transparency that allows external researchers to report vulnerabilities as they find them, right, unmitigated vulnerabilities. They are facilitated by programs like mobility disclosure programs.

We are seeing the trend for IoT security baseline, a focus on that is the capability and organizations are encouraged to have a very clear policy, that says if you find something, if you see it, please say something, please report it, to this channel. We will work with you collaboratively, to facilitate a remediation and a mitigation for the vulnerability. Especial when its to component that process of facilitating the remediation and developing the mitigation in a way that's tested, verified across ecosystem and increases patch adoption by end users often termed multiparty vulnerability disclosure process, is one where we collaborate very intensively with the ecosystem across the board. This is another area where you are seeing companies operating, not just of course the importance of cyber threat sharing information, working with the certs of the world and the ISOCs of the world and also facilitating the collaboration around the development of the mitigation for vulnerability, and working together to create a remediation that is actually getting adopted by end users.

So I just wanted to add that point, because this capability of vulnerability disclosure and handling processes is, in fact, one that we are seeing a lot of focus on when it comes to IoT security.

>> SHANE TEWS: So I'm looking at the questions and thank you, Mike. Mike has been multitasking and answering questions in the Q&A as we have been doing this. I really applaud you for that. But a lot of them are around open source. And what we're doing in that space which also brings many he to -- I -- let's start with that one because I have a question about content delivery networks. Michael Nelson says can the panelists talk about the role of open source software in IoT devices. Libraries of open source software are used by thousands of manufacturers and the code is very good and tested by great engineers but bad updates can sneak in, and so one is libel if something didn't work as advertised. What are the key developing and using super secure open source codes?

>> MICHAEL BERGMAN: Amit, I saw you smiling and nodding throughout that question. Do you have something to say otherwise I have something to say.

>> AMIT ELAZARI: Why don't you go ahead.

>> MICHAEL BERGMAN: So here's the thing, Michael brings up a very good point, and it's something that we have been concerned about and matching and talking to people about for some years now. About five years ago I had my first discussions with the open WR people at Purple Foundation, about what it would say to make that software more secure.

Not because it was a particular problem but they had a great community that was brought together by the Purple Foundation and this was a strong ability to message to that community. So this is a supply chain issue. Dealing with the Providence of your software and the software build materials. And what is happening is NTIA has been convening a multi-stakeholder process to develop a way -- not to develop, but to standardize on the efforts on modernizing software components at the very first level in your product and then when those components integrate something from something else, itemize those and this reaches all the way into the open source that you pulled in.

Now, when you look at a piece of open source, that open source software could be changed from day-to-day, because it's an open process.

Somebody could have snuck something in. Once you have picked up a piece and you vetted it and you know this is the one that you are going to use, what you can do is create a hash that verifies that this is not changed later on. It's a hash, a cryptographically secure number, that represents the exact code that was what you pulled down and developed and verified.

We're not there yet. Software build materials is not quite ready for wide scale across the board ecosystem deployment in my opinion. It's very close. There's been a lot of great work done by the stakeholder process at NTIA, Allen may be on the call. If you are on the call, you owe me a beer.

That's really, I think the main ticket across the board industry-wise. There's also secure dev ops processes that are intended to bring a piece of code in, vet it yourself, and then not always rely on something else.

Rely on what you know.

So those are the two things that I would mention. After the development process is complete, there's also certain types of testing that can go back and look for problems without necessarily knowing exactly what that problem might be.

Something called fuzz testing, where you just throw data that's randomized in certain specific ways at the system to see if you can get something to react the way it shouldn't. Now, I could talk more about that but probably that's a little too technical for a general discussion. So I hope that answers the question.

>> SHANE TEWS: Yes.

>> PAUL EISLER: I will add two things to that. First, the issue of liability, and open source, well, it is true that many cases it's difficult to attach liability to the person or entity that is introducing the update to the open source software. I mean, once that -- once the open source software gets embedded, into another system, in so far that's an entity that you do have a trusting relationship with, there's an assumption ever responsibility, in many cases explicitly in contract where there would be a way to hold folks accountable unless you really don't know who you are doing business with.

I want to also point out, I completely agree with Mike Bergman's assessment of the importance of the NTIA work. Allen if you are listening, you owe us two beers.

>> MICHAEL BERGMAN: No, no, that's two to me.

(Laughter).

>> SHANE TEWS: I would say, party at Allen's house. I don't know about you guys.

>> PAUL EISLER: While we strongly support what NTIA is

doing, there is still a conversation that has to be had about some of the ways that we can continue to evolve this process and the recent release of the SBOM minimum elements are we are encouraged it will be iterative and we are continuing to work with them because we think it's so important what they are doing we want to make sure that it gets done right.

>> SHANE TEWS: So just to throw more love on Allen, because it seems like we are having Allen fest. He's probably had the best use of time while we are all on lockdown on COVID. He has several things that he does that explains SBOM on YouTube. So I have interviewed him and I have been very impressed with how well he does it for an average bear. He goes from 101 to 301 and he has the whole twinkie analogy that he uses but it's a great point to bring up how, you know, you need to know what the next layer is especially when we are going to a software world where software is eating everything. Public service announcement, there's a healthy chat discussion if anybody is not watching the chat and I would imagine it's archived, and there's a lot of thank you to the panelists and other people that are adding pieces in here and we're having a whole discussion about this on the side.

And thank you -- Mike, you are doing such a good job of answering all of these questions by the time I want to ask them, you have complete them. Felix is asking what is the opinion about the panelists about using blockchain no secure IoT infrastructure? Anyone want to comment? Blockchain?

>> AMIT ELAZARI: While people are thinking, I want to add a quick thing on the last question and bring us back to what we started with, which is the importance of collaboration and public/private partnership.

The SBOM is one consensus driven process that is part of the executive order, I think, NIST is going to contribute to that as part of their development standards there and guidelines that are Section 4E and that conversation would continue and, of course, industry is participating very much actively in the conversation with the SBOM but that's one pillar of security and open source. What is important is we continue to facilitate those consensus driven processes and understanding, right, advancing our understanding of what it means to secure open source and part of what we are doing right there is participating in initiatives like the open source security foundation, where a number of private partners are together with others are, again, facilitating these conversations for issues like the SBOM but also for issues like vulnerability disclosure and or elements and processes that are relevant to secure open source.

>> SHANE TEWS: Very good point.

>> MICHAEL BERGMAN: I'm sorry, Paul, were you going to -- the focus went to you. Let me try to address the blockchain item. Thank you, Amit. That was great.

One of the interesting ways of doing that is making -- has to do with making absolutely sure that the software that you are running on your IoT device really, really, really truly came from the original manufacturer and is actually in line, exactly what they wanted you to be running. So that's great. Yay!

But let me sort of give you an analogy. I mean we're talking a little bit more about basic meat and potatoes security. We are not talking about filet mignon with caviar and truffles. So when you have the minimum job taken care of, and you start growing in sophistication, things like blockchain IoT certainly have a very important role, potentially. But in order to get to the point where the incremental benefit of using something like blockchain is important, by the time you need that last 3% or 10% or whatever benefit you want to quantify it as, you need to have taken care of a bunch of other stuff first.

Now, what we are promoting today, we're talking about today is baseline security. We have used the term, but if you go back and look up what baseline, you will find Amit's tech and you will find ANSI20-8 and NIST 82-59a and the CSDE Paul spoke about the CSDEC2 consensus.

All of those address the minimum baseline that everybody should meet. Even once we get compliance there, broad compliance more or less, we also need better development practices, secure development practices. Ideally, we would start with secure development practices but when things are bleeding, you put a bandage on first. So secure development practice are important, and secure development processes that substantiate those processes is very, very important. We have a lot of work to do to bring the ecosystem up to meet this challenge.

Blockchain, love it. It's very cool and interesting stuff. I can say the exact same thing about post quantum encryption and using quantum computing in the context of cybersecurity all of these topics are great but first we got to get the basics taken care of and that's what we are all about right here.

>> SHANE TEWS: So do you feel we are getting the basics taken care of? Where are we on the level of basics taken care of? Are we on the path?

>> MICHAEL BERGMAN: Do you know what it's like? Take a whole playground full of children, right? And you tell them go play soccer. And they have never played soccer before. Let's hypothetically. This is not a perfect analogy. What we have done so far is we have drawn the field. We have written up the rules and put them on a board. We have got referees going into place. That's the conformity assessment bodies I mentioned. We have organizers, that's NIST, that's CSDE. We have important well-respected players stepping on the feel like Pele, and that's Intel. We have all of these kids, and we have the kids.

>> SHANE TEWS: Interesting analogy. I feel like Amit should have on a Jersey right now.

>> MICHAEL BERGMAN: I want a whistle.

>> SHANE TEWS: We have two minutes left. Anybody want to do a last round of thoughts, where we are headed and where want to leave this group with this discussion?

Paul, I will start with you. It looks like you have words coming out of your mouth.

>> PAUL EISLER: Obviously, it will be important for government and industry to continue to rely on each other as partners. We're also going to need to continue to driving towards an international standard and do our best to mitigate regional fragmentation but finally, we will need smart policies to make it easily deploy security designed products in countries across the globe. This is not just a US problem. So you need to raise the expectations for security no matter where you live, no matter what language you speak. I have said it before, cybersecurity has no borders and we need global solutions.

>> SHANE TEWS: Fair. Adam, he's kind of put new that with governments being important.

You are big important government guy.

>> ADAM SEDGEWICK: Something like that.

Yeah, no, I was going to -- so I really appreciate the question and I think Mike addressed it well in the chat about cloud, and I think I would sort of echo that that's an important thing to consider. Another thing -- but another thing we didn't really talk about very much today is privacy, and I think -- and I think a lot of the facts that Mike brings up about the challenges with engineering good security are like 20-fold when it comes to privacy and particularly with IoT devices, you will have a lot of unique privacy needs that are very different than the security capabilities.

So that was something I would kind of put a pin on and situational awareness let's talk about work that we can do to get true privacy engineering practices pushed forward. We do work in that space but it's something I think we need to do a lot more around and on.

And I would agree that this is, you know this is something that regardless of what paths, any sort of policies take, there will be a basis and there will be a necessary basis of strong public/private coordination or call it public/private coordination depending on the types of issues we are trying to address.

>> SHANE TEWS: Amit. Final thoughts?

>> AMIT ELAZARI: Yeah, my final thoughts are, I mean, security is not a one-stop step. It takes all of this and this is what we are seeing. And if security is, of course, top of mind that it's a critical issue and a priority when it’s to IoT and security across the board. It's not just about the technology. In the technology, it's not just about our, you know, best assurance, SDL, processes, leading, vulnerability discloses and it's also the foundational security in the hardware, the software across the board. It's also about the partnership and the partnership is everything from enabling the ecosystem and it's the active participation, the collaborations through alliances through work on technical standards and it's advancing our shared understanding all the way to participation with governments, with policymakers and those public/private partnerships and it's also collaboration and partnership with the security research community, as they work and, you know, uncover the vulnerabilities and the issues of the future.

So for me, the real take away from this discussion is the importance of collaboration, the importance of flexibility, and working together on all of these documents as we are trying to tackle the emerging attack surface.

>> SHANE TEWS: A lot there. Mike? Final thoughts?

>> MICHAEL BERGMAN: I will be very quick because we're at time. I want to thank Shane, great job, and my fellow panelists and just say to anyone out there who has policy somewhere in your job, what we described today is a framework that starts with a government agency and their fundamental document, works through levels of sophistication or refinement

or different parts of the chain, all the way out to verification by third parties and self-attestations, verified by business-to-business relationships, all of this should be watched very carefully by anybody who is thinking about policy for IoT in Washington and quite frankly internationally. It's a complete soup-to-nuts picture. And we consider IoT security in their own context, you know, what is the relationship of cybersecurity for product. So as agencies and other regulators and legislators consider IoT cybersecurity, please, please, please, look at what is being built. Don't start from scratch. Don't try to do something in parallel. Don't go to some outside organization, this is industry and government working together. It works. Take a look at it. Try to see if you can hitch on to this train. Thank you.

>> SHANE TEWS: Well, thank you to all of the panelists, not only for today, but for all the work you have done and all the work I know you will continue to do. So as somebody who loves all of my devices and I have lots in any house but understand that we have so much more coming online. The work you are doing is amazing. So keep it up, and Dustin, back to you.

>> DUSTIN LOUP: All right. Thanks, Shane. And thanks, everyone, for a great panel, and rounding out our morning of security on a strong note.

So we're going to move into a quick break before transitioning into our next session and the topic of privacy. So go ahead, take a quick break. Just a reminder that there is a networking room open, and our friends from the Dynamic Coalition will be in there for this break as well. So we'll see you all back here at 1:30 p.m. eastern daylight time, and enjoy your break.