**Project Completed by:**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

**Selections from the**

**EDUCAUSE Security Professionals Conference 2018**

**August 21, 2018|12:00 - 4:30 PM EASTERN**

>> Hey, Randy, so we're back in our next session. Zero trust networks, the future of higher Ed security network design? Welcome Randy, we're so glad you could join us today. Please fell free to begin.

>> Thanks a lot. I hope everybody is doing okay. I always like following Joel, because I go jeez, why didn't I think of that before? And he and I, I think, we're right around the 40-year mark at our institutions. So what I want to do in this talk is basically, kind of walk you through an architectural concept that most of us have embraced parts of in our careers, we never gave it a name. And to make you think about how the Internet itself is changing. So I always like to start off with this slide, I do this when I talk to the corporate guys and they say, you guys are different from us, no, not really. But our challenge is we have to balance three security models. Every university, every college, every EDU has three business processes, and the first one is the administrative one. That's the stuff that runs the university. Payroll, HR, facilities, legal, all of the stuff is in there. And that security model in the traditional sense has always followed more closely to corporate model. The academic instructional side of the house, that's the -- you know, course management, learning management, examples are shown in the bullet points there. We use zoom, some of you use black board, noodle, canvas. For us, web X, all of these types of things, but this is a heavy BYOD environment, this is where I like to freak out more corporate -- my corporate counterparts. It's not a big issue for us, we've been doing it since 1984, where have you guys been? But the security model is more of -- is closer to that of an ISP. We don't tell people what they can or can't have on their individually owned machines. But we do have a requirement that they meet certain minimum-security standards before they connect to our network. For those of you that are research universities, well, your hybrid of the first two business processes, the administrative piece is more intellectual property protection. And the security, you know, the research piece of it is where we build our own devices, we bring in data acquisition devices, or data analysis devices that have to connect to our network. So this is -- these are the flee models that -- business processes that security times most EDU, have to figure out to balance. In my other life, I worked in the -- teach at the sands institute, one of the stands instructors, I get to work on these projects with them and every five years or so, we look and take a look and see what are the goals of attackers. What I discovered in the 30 years that I've been with sands is that really, the attacker -- hackers attack, they do three things, one of three things, or all. They're after your data, either to steal it or to disclose it and otherwise, known as data breaches, or they want to use your assets to attack other sites. Back in the 90s, and in the early 2000s, this was the biggest complaint against EDUs, you guys are so wide open, using your machines to attack us. That's the second thing here. And then, the last one that has resurfaced again, is the ransomware, we're going to destroy your data. Now, whether that's done by an insider or by a blackmailer, doesn't matter, that's what they're after. Ransomware is not a new thing. Ransomware is I think the first one was in 1989. With the first ransomware attack. The reason why it's more popular now is of course because of bitcoin. You know, in 09, the state of Virginia was a victim of a ransomware attack, 2 million dollars, in a suitcase by a mailbox by a street, you're going to nab the person who's picking up the money, but with bitcoin, that's going to change the rules. What we have to do is we have to realize that they these are the things that hackers do. We have to not worry about the other types of attacks, this is what the majority of the attacks are up to. Those of us on campuses and things like that, land grant universities, like us, we have our own power plant, it's in the grid. Electrical grid here, provides power to the campus as well as the surrounding town. We have police departments, we have, you know, cultural activities, we have housing, in terms of dorms, we have restaurants and food services, in terms of dining facilities. We have traffic monitoring around campus. We have all sorts of the aspects that you would find in a small town, we have on our campus. We may not have realized it, but it's there and all of this is now networked and so we have to consider these things as we build our new security models. So my buddy, Christian, who used to be at the University of Arizona, now with fire eye, we were talk about what EDUs are like, I use the small town thing, but he said, you know, EDUs are like museums, we have to allow a lot of visitors to look at our assets, but we also have to protect the assets. And so, you know, more valuable assets, we want to make them accessible, but we certainly want to make sure we know who is inside of our building, and so we covered the interior thoroughly, and we assumed that there are bad people inside of our buildings, so we want to take a look and make sure that we know where they're going. And so, you know, this little diagram here, thousands of people see probably one of the most, you know, valuable pieces of art in any culture, you know, the month NA Lisa and thousands and hundreds of thousands of people can get into the building, and view that, they can't get close to it, it's well-protected. We have lots of, you know -- very similar to a museum. We have a limited number of access points. But they are free-flowing. You know, for the most part. I grew up in the Washington, D.C. area where museums were free. You know, so. But I mean, you have these free-flowing access points and then we have barriers around the high-risk things, physical barriers, we have cameras, we have all different types of things. Motion sensors. You know, museums have physical guards, well, we don't have that around our banner machine, but we do have a police department and we do have rescue squad services and things like that. And in terms of recovery, cyber insurance is one of those things now that is really catching on. And we do have ways to track files and sensitive data as it moves around. If you're wondering how that's done, Google for web bug. You can web bug sensitive documents or sensitive files, and use that as a way to help you track things. But the primary assumption, and I think this is true for everybody in the EDU community, where I always like to, again, my counter parts in the commercial world, I said, look, we assume that they're already inside of our network. We assume that the hostile people are inside of our network, and we go looking for them. You think they're not in the network and I tell the corporate, the corporate counterparts, the reality is that they are. So how do we come up with a new model to protect us? Well, these are the goals, this is what we are trying to answer and Joel covered a lot of these in his GULP talk. But you know, can you name the assets that you're defending? Do you know where they are? Can you see them over your network? You know, can you detect any unauthorized activity aimed at those assets? You know, can you classify your -- what you detect? Can you decide this is a serious threat or not? Can you identify the adversaries or at least where they're attacking you from? They may be spring boarding through another domain's network, but can you notify -- this is the question I have for you. Guys, if a machine at Virginia tech, for instance, is -- you detected an attacking machine at your campus, do you send a notification letter to us at Virginia tech and let us know, hey, this IP address in your network is attacking us? And you know, curious just to see that. I don't have an online poll, but you should notify whoever is -- whatever domain is attacking you that you detected them. Also, then, can you see what the activity is inside of the environment? What are they doing once they're inside of your network? Can you hunt them down and isolate them out? Can you track what they're doing and can you act? These are different levels of incident reupons and how you protect sensitive data. But you need architecture that can provide those to you. We think we have that, but most times we do. Well, is this just BeyondCorp? And hunter will be talking about that. These are the characteristics of both. Pretty much the same, all the way across. Although, and BeyondCorp is more managed device. BYOD is a big challenge. But again, with hunter's presentation, and Mike's presentation from Stanford, they've done some really, really interesting work oncoming up with host-based inventories. So this is what we're up against. I like to -- I like to sort of twist the Internet version numbers. The Internet of the 70s and the 80s and pretty much most of the 90s, it was static on both ends, the servers were static, the end points were static, you had a desk top, a mainframe server. Internet 2.0. The advent of laptops, servers were static, still mainframe things, rack mounted servers, but nonetheless, they were static, they were in a data center. But the mobile end points, we started seeing people move around in the networks, new protocol, wireless protocols, started to come into -- become mature technologies. And so that's what we see. But really, where we are right now is in Internet 3.0, where the mobility is on both ends. The servers are mobile. They're containers, they're server less, cloud based, where the cloud is on PREM or off PREM, doesn't matter, they're mobile. As well as the end points. And the laptops, the phones, the tablets, the IOT, the industrial things on the campuses, both ends are mobile. And the traditional architectures that we've got today aren't geared to work in that type of an environment. Where we are right now, most cases, we're stuck somewhere between the Internet 1 and 2, so we need to go to Internet 3. This mobility issue is a big challenge for us. So that's why we -- I started looking at this and ran across this book. So I wanted to talk a little bit about zero trust networks, this is an architecture presentation, we're not going to dive into the details, there's references in the slides that give some more details on this. But the idea here is stuck with me for their characteristics. And so at Virginia tech, when we built the network, we just always assumed it was hostile. And we always assumed that they were already inside of our network. And so that type of -- that type of mind set for us, is one of the reasons why, again, those of you who know me, the border was not the border in the traditional sense, it was the device. I've not modified that, you'll see how I've modified it in a minute. But we've always assumed the network was HOL -- Hoss style. Snyder -- Snyder network. For deciding trust, it's not so much -- I'm not talking about access, I'm deciding who is allowed and who is trusted to be in the network? And this locality or segmentation thing is not sufficient for that. It comes down to where you have to come up with a way, the process, to authenticate and authorize every device, user, network flow, Stanford has done some really cool stuff in this arena. And again, like dynamic environment like everybody else, and so we have to have our policies that can change and adapt with that. Because the devices no longer the border. A user's identity is the new border. EDU roam campus and log in with my regular credentials. We've seen this now where you log into vendor services and they say, user FaceBook or user Google credentials. The authorization piece isn't sometimes in your own -- within your own network borders and ultimately, it comes down to data. My job as a CSO is to protect sensitive data and do the best we can do to keep sensitive data from leaving our network. We want to make sure we don't violate any data breach notification laws. I've said this before, there are no device breach notification laws. There are data breach notification laws. And so consequently, why not make that the new border? Container and serverless and cloud computing, these are the new disrupters, we're struggling right now with how do we doic -- forensics with con -- containers. Well, you have to do more logging because I now depend on the ability of your apps to send information out there. So this mobility thing, the mobile users wireless, mobile apps, mobile storage, that's one of the reasons why we have to move in this direction. So all the data, sensitive data, let me qualify that for us, right now, but certainly, the goal is all data has to be secured regardless of location. For us, practically speaking, sensitive data. If it's got social security numbers, credit card numbers, passport numbers, bank or debit account numbers, that's sensitive data, it has to be approximate -- encrypted at rest or in transit. Store nit the cloud, if you encrypt it with you own local keys and you put that encrypted file in the clouds, go for it. If you want to put it on a USB device or some type of mobile storage device, if it's encrypted with your keys, and your individual keys or organizations keys, it doesn't matter to me. But if it's encrypted and you put it on the devices, go for it. You have to have that type of a guarding. If it's public data and you put it out in the cloud, so what? If it gets access without your permission. So the trick here is, you know, we used to talk about trust, but verify, but the zero trust model is the flip of that, verify and never trust. And so what this does is we get rid of this inside prim administer stuff, and the trust is where it needs to be, at the new border, the user or the data that's there. So some quick components of it, and this is from Government computing magazine. This is one of the guys in one of the cabinet departments talking about how they have to shift over to follow the user. The policy has to follow the user, no matter where they are or what device they're using. So in other words, data is the border here. Okay. So we treat all hosts as Internet facing, always like to, you know, go n a-na-n a BOO BOO. That would be terrible anarchy. But at Virginia tech, like with Columbia, all of our nodes are Internet-facing, they're addressable. Access to them is controlled by host-based firewalls or localized structure. But they all have addressable, you know -- we have other things, but for the most part, there's that way. It's a perfect thing for the cloud. Sorry. A delay here. So we have two planes, we have a control plane, this is sort of the user device authentication, authorization, it's done here, this is the service -- these are the services that connected authenticate authorize a connection, if you will, to network resources. And so that's the controlled plane. The data plane is the physical stuff. The applications, the firewalls, all of the stuff that process network traffic. All of the devices that do that there. So a typical interaction in a ZTN environment, is a client, a server, you have a control plane, the client requests access to the service. The service, you know, checks the control plane checks this out, it reconfigures the service to allow access from the IP address of the client. You get this temporary access configuration. And then, you can connect to the machine. Okay. And so you know, we had these types of agents. And, you know, they're formed on demand. Again, the authentication is done before the formation is set. You want to put this enforcement mechanism as close to your end points as possible. And you know, your microsegmentation of a network, I suppose, if you want to think of it that way. The policy engine makes the decision. And then, you know, use certificates, X.509 certs. An example of how you would do this. Where you trust the devices. Softwares, we use CIS, the center for Internet security benchmarks to help us create a spore. The BeyondCorp was a pioneer in this area. If any of you have done anything with the critical security controls, that's control number 1 there. Multi-factor authentication is a typical one there for authoritative identity, authentication, we use DUO, all, faculty, staff, student and alumni using DUO, over 150,000 users. We did the switch, we switched everybody over back in 2016. Network filtering, and authentication, how do you do this type of device authentication and thing we're talking about? There's a whole concept called single pack, packet authority, SPA, a link to it there. Not going to go into that detail. It's similar to port knocking for the techie, but there are differences where you put everything inside of a large data packet. And so, again, you know, you want to filter PLS, again, for application protocols, basically, what we're saying here is encrypt your traffic as much as possible. One comment I always see is people say I need to expect the traffic to see if I have a data leak. No, this is where threat intelligence comes in. If any traffic to a bad domain in the clear or encrypted, it's bad. If it's going to a bad domain. So once again, you want to look at your network flows. Network flows are a key component of our network forensics, architecture, you want to be able to use that information as well. Use your strongest authentication -- authorization and encrypt protocol, you have to have a PKI system in place, we've had one since 2003 or 4. I know of a bunch of other institutions have a PKI infrastructure for that. If you want a CR, you can go to -- see ours, you can do to PKI.VT.EDU to see what we've done there. So my suggestion is build a small department -- and try the zero trust network principles to it. Build a system and diagram, do you know where your inbound traffic goes, do you know where your outbound traffic goes? And this is a real key for us. So as an example, we profile net flow connections. And we broke it down by countries. This is just a sample one from 2017. The blue is what comes into our network from countries, and the United States is shown there at the bottom of the slide, I took it out because the numbers obviously -- the Instagrams would be tiny things. But typically, what we've seen in this particular graph, we're looking at China, Russia, Great Britain, Mexico, Netherlands, France, Brazil, Korea and Canada, we see a similar pattern, more coming in than leaving our network. And that may surprise people. But a lot of this might be, you know, if you're doing web searches, you know, you're going out to a Web site, typically, you know, you type in Randy Marchany, that's a small outbound packet, you get a back a bunch of results. This is a pattern that you would see of normal traffic. If you see more coming -- if you see more leaving than coming in, then perhaps that's a problem. Or maybe it's a research institute that's doing some stuff there. So sort of wrap up, I always like to -- we're in the middle of implementing the 20 critical security controls, so zero trust networks basically, you know, address controls one, the hardware and the software inventory, configuration for log -- for devices, log analysis, malware defense, boundary defense. If you have any of these particular things in place at your institution, you already have a piece of zero trust networks. And then, wireless access control, more monitoring control, you notice that these are more on the logging side of things. So you can't go out and buy a zero trust network right now. There’re still pieces of it that are still, you know, in development and things like that. But we have most of the foundational blocks to start approaching our building a new architecture, that's what we need to do is we need to change how we have built our new security architectures to address this new mobile -- mobility issue on the server and the end point side there. Because data mobility and protection is the key and then, these are going to be the things that we're going to have to deal with, they're here, we have to deal with it. We cannot prevent them, we have to learn how to adapt to architectures to deal with clouds, containers and serverless apps. These are references, any quick questions before I finish?

>> Thanks, Randy, we have one question that I think we have time for. So e-mail seems to be the weakest link, how are you handling e-mail?

>> For us, we do have out look exchange, one e-mail system, but everybody -- we use Google apps for education, everybody has got e-mail -- gmail account. And we give up some, you know, control to Google, but that's where we are right now. And again, as long as you can access logs, you follow the Columbia concept, that's a big thing of control there. And once again, if e-mails vector to get in, at least you monitor your outbound traffic and you know if somebody got compromised. I'll take questions on the chat window as we move on with the presentations. But thanks a lot.

>> Thanks so much, Randy, for joining us, and we're going to take just a second or two to reset the stage and as Randy mentioned, you're welcome to add your additional questions in the chat and he'll try to answer them there. Thanks. [Please stand by for webinar to resume]