**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**

>> We'll kick off the second half of today's program with today's talk. Joining us is Michael Duff, Chief Information Security Officer at Stanford University. We're delighted to have you join us. Please begin.

>> I think this is going to be a great compliment in what you heard in Randies presentations. We're doing something at Stanford that today is exraw ordinary and will become the norm for all of us. Improving user experience. What I'm presenting today is a culmination of five years of work but it won't take you nearly as much time because in my experience the bulk of counter time spent on large scale projects like this is usually consumed by design decisions try and error and concerns about efficacy. In other words, if someone handed you the finished project with final results and said implement this you could do it in a fraction of the time. And implement. I hope sharing our journey with you, you too can go passwordless. Throughout the presentation today I've highlighted decisions with yellow stars because again I feel like we spend a lot of time in arriving at those decisions and just wanted to call those out for you. This very began back 2012 and if I had a vision using device applications. Kind of like what you heard in hunters presentation I knew there were a lot of building blocks that we had to put into place. I knew to get started I was anticipating a campus wide roll out. Well, circumstances intervened to accelerate that rollout. I think all of us can consider incidents, a major breach we had in the summer of 2018 which propelled our rollout and in fact we were aable to rollout rollout in about six weeks with no exceptions and that was back in the fall of 2013. Very pleased with the results of that and we've transitioned to duo since then and so that was one of the building blocks. Well, around the same time we had a series of loss and stolen laptop computers that contained unnen crypted medical records which lead us to try to compel everyone to in crypted but we knew that policy alone wouldn't cut it. If it's opt in -- we built this tool to integrate several systems of record to innovate viewpoints so finally and this we rolled out in 2014. We finally had a view of who is using what devices, what their affiliation is and what their device security posture is. One of our enforcement mechanisms is campus network access. We give people a thirty-day grace period and they know by getting notifications from my devices, at any time they can go to my devices dot Stanford dot EDU and understand what's been registered to them. Our encryption rate, our enterprise risk management program lost and stolen devices that are un in crypted you went from one of our highest risks to one of our lowest risks so this is very successful. But there's still some gaps that this leaves. One, some services don't support two factor authentication so we don't get the benefits of that. Second, many devices never use our campus network so they are not subject to the enforcement imposed by my devices. So that brought us to what we think is a solution. And it's device-specific user certificates. So I'll explain the idea and then we're going to talk about the architecture behind this. The high-level ideas that each endpoint that we have gets it's own digital certificate. It's not new. It's been around for a little more than forty years now and it not only authenticates the device but it authenticates the user who is assigned to that device. In fact, I'm convinced that this is the right approach. It's similar to beyond Corp and what you heard earlier. Sometimes I think of it as beyond beyond Corp because it actually involves identifying the user as well. Why are we doing this? Well, number one is stronger user authentication, right? We want to make sure that we know who is using what devices and that we can feel secure about that. Next, the course is fishing which is the number one security threat today. We have compromised credentials and third, we need to know that even if a device is not on the campus network we need to know what device that is so we can corollate that with who is using it and finally, last but not least is the user experience. And this is one of those rare situations where we can improve the user experience and security at the same time. I'm not much of a salesman but here's my sales pitch that I usually start off with presentations on this topic. Imagine not needing to enter your password anymore and yet be dramatically more secure. Well, that's what this does. Step one in this whole thing is getting a certificate. We knew we had to make sure it was easy for people to fetch and install certificate. Certificates have come a long way in the last forty years primarily not in the algorithms but how easy it is to deploy and manage. We have this four-step process. You can get a certificate in less than sixty seconds. You do our web single sign on. I put a star here next to duo. Finally we use a cloud based cloud path that will generate the certificate and help you get it installed. Here's had what it looks like. You go to beginning this process and type in the device name and hit continue. And then it prompts you to download the executable and that sets up everything for you and you are done. Alright? Now we're kind of lucky at Stanford that we have very few integration points. Authentication is highly centralized here and we're lucky in that sense, but our main three points are VPN, sign on and secure wireless. Let's take a look at what this looks like in the old approach and the new approach. The old approach looks like this. You begin by hitting the connect button in the in connect client and then you do your username password followed by a two-step authentication and then there's a little message here and then you are connected. It takes some time. With certificates we've shortened that down quite a bit as you can imagine. With our certificate set up you open any connect client for VPN, click connect and you are done. You'll notice that we eliminated the two-factor authentication step and that was a decision we made also with user experience in mind to streamline it because the VPN really gets you on to our computer network and we do not skip this step for application log ins. The way it works today without certificates is web single sign on using username and password and we require doing a two-step authentication every ninety days and then you are logged in. Well you can probably guess what this looks like with certificates where you basically skip that first step of username password. We still do two step duo authentication every ninety days. The vast majority of the time you don't see a log in screen. Let's tune into the architecture of all of this. What I'm showing you here is the conceptual picture of where the web single sign on authentications sign-in without certificate. Log into the VPN and checks it against the revocation list and it makes sure the username is still valid and every ninety days it prompts you for two factor and step seven is key where it calls out to my devices and says, hey, what's the compliance status of this device and if everything is good it says we're good and you are logged in and given the assertion to be able to log into your web service. Well, this looks great but there's a couple problems here that we realized. I circled them in red. One is the certificate revocation list checks. There's typically a high latency and it ends up being a single point of failure. Next is a failure with my devices. We didn't design it to be a transactional system. We designed this like I'm showing now and really the key point here, the yellow star is what we call a certificate cash. It knows the device information and it combines a certificate status into one and certificate cash is built into our IP. You have the database connected to it and it's high availability and all that is taken care of so we don't have to worry about the transaction rate or availability issues. This is actually our architecture that we set up for this. Let's move on to talk a little bit more about the certificate cash because it's interesting. As I mentioned, high availability, built for high transactions and it's built in and has a rest API that we built and we call that from my devices and cloud paths because those are the other systems that are full of information or certificate cash interface. You might not think so but the certificate hierarchy design was -- we actually agonized over this for years. It took more than two years to finally decide on our hierarchy and that's why it has the design star on it. Three tiers and then the actual user device certificate which you'll notice is good for five years and I know that's somewhat unusual for user and device certificates. Typically, it's one year but one of the lessons I learned from previous implementations is that that ends up being a management nightmare if you have to renew certificates all the time, and so we wanted to avoid that. You'll notice that the user and device certificate has user ID and device ID and it has an e-mail address of the person. It's a little redundant because it includes the user ID but it's important to have both in there. Here's what our route certificate looks like. Here's the route certificate. Here's what our intermediate at certificate looks like. And then here's my actual user and device certificate for one of my devices. You'll notice this enrollment/long string is the identifier that's unique to that device. Well, you might wonder, what did we use to create the certificate hierarchy? Did we use a system like active directory Microsoft certificate authority service that has a lot of this stuff built in? For a few reasons we decided to do it ourselves. We actually conducted a formal C A ceremony and we did the whole nine yards. We picked an undisclosed location. No one knew where we were going to be and when we got there I decided at that moment to change the location so not even I knew where we were going to end up. We recorded the whole thing through zoom. We of course muted during the times we were typing key strokes like passwords so no one could do audio analysis on it. We used a raspberry pie to generate all of the keys and we actually rehearsed this and planned it for an entire year and we had ten pages of instructions and it ended up taking ten hours to get through the ceremony. Here's some of the key points in the key ceremony. We had four key masters as a designed decision to ensure redundancy in case someone left of the University or became incapacitated. The goal is to generate private keys in this case. Generate a key wrapping password and we split that into six pieces among the four key masters so no one had all four pieces and if you look here you need at least three key masters to re assemble the key and we in crypted the private key and split it up in the six pieces again similar to how we split up the passwords but we were later informed by our photography experts here at Stanford that's not the best way to do it and we should use a secret sharing algorithm so that was one of the lessons learned from this. We ended up with our C A key intermediate at and the intermediate at can generate the device certificates. This is the part I'm most concerned about. The route I'm not worried about. It will never be online and that's in good hands. Our intermediate at C A key has to be somewhere where we can access it. We put it in cloud path and that's how certificates are generated. I want to touch on here a little towards the end, one of the challenges that isn't immediately obvious from this and you really have to think through it to understand why this is a problem, but the key issue was how do we associate the certificates that are generated with the devices that they are on? It turns out that that's not as easy to do but because of our prior work for my devices it turns out each of our endpoints has an agent on it which can tell us which device has which certificate on it and that allows us to make that connection between the device and the certificate. Where are we in our deployment? Well we're in year two. Year one was building the infrastructure and year two is the adoption and that's what we're doing right now. This has been rolled out for VPN, one single sign on and ready and it works. We tested it and we're actually going to roll it out beginning on September 20 th and the third year will be to require a third base authentication. When I think about this project and what we're trying to accomplish three words come to mind and that's quid pro and quo because we want to provide incentives for people to adopt us which is a better user experience through simplified log ins and pro infection against fishing but we also want to get something out of it so we are actually requiring that in order to play you have to have an endpoint agent on your machine and that your device must pass a security check before you can access Stanford. Here I've designed key decisions along the way. The slides are on the web and you can refer back to these but these are ones that we agonized for years. Here's lessoned learned. I talked about the calendar time and that's consumed by design decisions and implementation has been wildly successful. It took a lot of work to do it, however, so I would recommend if you are starting from scratch use Netflix stethoscope or duo has offerings in this as well. Finally, the gifted power of that good user experience can have. Here's a list of some of our resources that you can find on the web about having to do building blocks of this whole system. And I wanted to end about three minutes early, so we have plenty of time for questions. I'll stop there.

>> Great. Thank you so much, Michael. It's a very he informative session and I know you had to condense this down from a longer talk so we appreciate you sharing as much as you could in this time. Shawn was asking how do you handle personally owned versus institutionally owned processes? Barbara asked how do you handle host or stolen machines or machines that you LendIt out?

>> We made a point early onto not make a point between the two. Any endpoint whether it be Stanford provided or B Y OD is treated the same way and you have to have an agent on it and now you can use certificates to get into services. Lost or stolen machines, the way those are handled with certificates is we can revoke the certificate immediately. We do require machines be in crypted and have a screen lock. More than 90% are in crypted and when they go missing we can revoke the certificate for that machine but either way they are already in pretty good shape.

>> Thanks.

>> Do you have another question? I see that question about shared devices. That's a great question. For shared devices, fortunately we don't have too many of those and we're actually on shared devices you would only have a device certificate as opposed to a user certificate unless you can divide those up by profile. If if it has a shared profile capability then no problem.

>> Thanks. I was going to say [Inaudible] University is asking what do you use for the device agent?

>> For our mobile devices we use air watch M.D. M. And for laptops and desktops we use IBMs big fix. We have another one that we built at the request of faculty. It's called valor. It doesn't modify the machine. It just provides the device and compliance status.

>> Great. It looks like we need to wrap this up so we can move on to the next speaker. I do apologize because I see there's a couple more questions. Michael, if you can respond in the chat there's questions. I just want to thank you again for your talk and we're going to go silent for just a moment while we reset the stage for the next presenter.

>> Okay. My pleasure.