CCCCO System-wide Architecture Committee (SAC)
Meeting Minutes
Thursday April 27, 2017
Zoom Online Meeting

Attendees: Tim Calhoon, Bob Hughes, Paul Bishop, Dave Fuhrmann, Rico Bianchi, Sylvia Lynch, Lou DelZompo, Jeff Holden, Bruce Racheter, and Caryn Albrecht.

Call to Order:

Tim Calhoon called the meeting to order at 1:35 pm and took attendance.

Minutes:

There were no additions or corrections to the minutes for February 23, 2017. Paul Bishop moved to approve the minutes, Lou DelZompo seconded the motion and the committee approved the minutes.

System Updates:

CENIC Update:

Tim reported there were a couple of months where not much was getting done, but after a bit of a "to do" everything is now back on track. About thirty circuits have been ordered in the last two to three weeks. The Technology Center is tracking closely to make sure everything is moving forward. There are about 235 circuits in use with 139 upgrade candidates. Circuits have been ordered for 80 deployments in progress and 26 circuits are completed.

The CSU has been acquiring dark fiber and it has gone well. So Tim is looking into doing the same thing in places where it makes sense for the CCC. They are also looking into special construction for colleges in more remote parts of California to get better connectivity.

There will be a mini grant for colleges to use in any way needed to better use 10Gig connectivity being brought. Most colleges are using it for upgrading their firewalls. Colleges can sign up for that mini grant on the Technology Center website, Mike Tucchillo will work with them.

Tech Center Update:

There are now just over 4M system wide student CCCID accounts and there is less a less than three-tenths of one percent duplication factor on those accounts. Federated ID Proxy is rolling out, with about seventeen colleges in production, eight testing in pilot, and an additional twelve in kickoff. Proxy is there for students who don't have a CCCID. It enables them to retrieve or create a CCCID and only needs to be done once.

The system just got through 5.5M applications for admission with CCCApply and there is a big push in the coming year for more BOG fee waivers and more International applications. The March CCCApply release went well and includes new items for homeless youth and a redo of the interface for OpenCCC so it looks more like the MyPath portal. Centralizing branding for a common look and feel is being done with all of the system wide tools.

There is a big move happening from Rackspace into Amazon for CCCApply and OpenCCC. Infiniti is working on that with attention from Lou and Jeff. It is being done in two stages. The first stage was a move into pilot for two weeks and later into the production environment. The pilot is in Amazon now, with no complaints. The move to production is scheduled for May 12th.

The MyPath portal is live at Santa Rosa Junior College and is being implemented at another six colleges over the next ninety days. MyPath has Career Coach embedded in it so students can take a career assessment and search for careers and programs for themselves. There is a new release coming out in April that will provide graphical elements the Chancellor's Office wanted for their version.

The Hobsons deployment which includes degree audit, educational planning, early alert, case management, and scheduling elements is currently live at seven colleges. Nineteen colleges are implementing the Early Alert component right now. There are another fifteen that are implementing the Degree Planner and another six with pending kickoffs. The goal is to take care of all colleges that don't have a degree audit/educational planning system.

E-transcript California includes 120+ institutions in California. Lou has been working on Postsecondary Electronic Standards Council (PESC) EdExchange work. There is a PESC meeting coming up next week. Work with EdExchange involves OEI with Ventura and Foothill-DeAnza and Parchment. Once a student has done their OEI course, the transcript will be passed back to the home college through EdExchange. Lou reported that EdExchange work is going well. There are three separate pilots going on: the transcript vendors have one of their own, there is a pilot with University of Phoenix, and then this pilot with Ventura and Foothill-DeAnza. Lou noted they are in the development stage right now so nothing is being transmitted but the intent is to pull together efforts with the OEI Course Exchange so when a student completes a course, the credit will automatically be passed from the teaching college to the home college; right now that is a manual process. There is a lot of positive potential in this for all transcripts, but for now OEI is their short term focus.

Lou thought work was being done with the same model as Ventura and Foothill (which are Banner schools) to do a second similar pilot with Colleague schools and another sort of bootstrap pilot supporting Colleague schools working with Credentials, they are trying not to be limited in scope.

The Chancellor's Office Curriculum Inventory (CO-CI) and C-ID rewrites are rolling out between now and June. CO-CI will be rolling out in three cohorts of colleges and C-ID will be rolling out as well.

Canvas is at 104 colleges with another four to six in the near future. Some development work is going on related to saving Canvas data into the data lake for learning analytics; Lou has a team working on that. The California Virtual Campus (CVC) is being rewritten into a version that works better with the portal. There are five colleges live in the Course Exchange: Fresno, Lake Tahoe, Coastline, Ventura, and Butte. Acceptance testing is also going on at Foothill. The big lift for that project will be inclusion of financial aid requirements, which is still being worked on.

CCCAssess Beta is still pushing to move out to twelve pilots in the fall. They are deeply embedded in testing items and as of today have delivered about 20,000 tests to gather data to validate tests and all of the items in the tests. All of that analysis and data has to be written up into an assessment test approval package and submitted, so they are on a pretty strict project schedule and deadline. The CAI also just went through an RFP for a machine scored writing sample. Vendor selection should be happening soon.

The proof of concept for the data warehouse/data lake is complete. Lou's group has done work on putting data in and pulling out into a data warehouse. They are just waiting to work with partner Ed Results on building out the DataMart.

Project Glue:

Project Glue is live in the OEI Course Exchange with a limited number of students that participated; it is live and works. CCCAssess is coming on-line in the fall so they have Glue adaptors developed for seven colleges and are waiting for the application to be live. The next version of Glue is scheduled for the fall. Support is being added for financial aid transfer in Course Exchange. Support is also being added to Canvas for auto-provisioning student accounts once the student is enrolled and finishes matriculation at a college; that process will honor guidelines from the colleges about when the student gets access to their course shells.

The Glue team is working on a set of information for later release that would pull data out of Canvas and make it available to the colleges either through the data warehouse, or some other mechanism yet to be determined.

In CCCAssses, the next version of Glue will also provide support for a faculty member to provide feedback on validity of placement. If a student was placed in a particular course, the faculty member would have the ability to add their opinion on whether or not they think the student placement was valid or not. This will mean bi-directional help for assessment.

Accessibility:

The Technology Center is in the middle of the hiring process for the Accessibility Director position. There is also an effort with the Chancellor's Office to have a Governance Committee for Accessibility; both Theresa Tena and the Technology Center are working on that.

Data Governance:

There is also a Chancellor's Office effort to set up system Data Governance and a Data Governance Committee to set policy. They will probably be approaching CISOA to solicit representation for data governance. There will also be a Data Governance Office out of the Technology Center that will help projects meet policy. They will also help enforce policy so the system will have better data which all ties together.

Security Center Update:

The Summer Workshop will be July 24-25 at Mt SAC and will have a bigger venue with at least 100 spaces. Jeff will be putting out a call for presentations; anyone who is interested is encouraged to email him.

Tenable Security Center is off the ground with a big push to get twenty colleges started. Tomorrow Jeff will do a video walk through to get colleges set up and then will start to have group install sessions once a week. Splunk installations continue to go on, but that is a little bit more involved. There are now sixteen colleges implementing. There are about thirty-five districts signed up on the unlimited SSL certificates.

The security team is just about finished up with security assessments for LACCD. There is one more school to finish and then Jeff will get their report out.

Chancellor's Office Update:

The TTAC Retreat in on Monday and Tuesday of next week. Next month Tim and Paul will bring back a report on what happened. Hopefully, the minor revisions made to the SAC Charter will also be approved.

Vendor Presentation Palo Alto Networks- Security Platform:

Anton de Leon, Account Manager- North Bay; Mike Jacobsen, Vice President of Product Management; Spencer Mitchell, Systems Engineer; Christian Romero, Account Manager- Central Valley

With the CENIC network upgrade taking schools from 1Gig to 10Gig networks, many colleges will be looking at buying new firewalls. Tim brought in Palo Alto, which has a firewall product to provide a vendor demonstration. If everything looks good, SAC may ask the CCC Foundation to work on a pricing contract for the system with Palo Alto Networks.

Historically environments were very static with users sitting at their desks, data centers oriented on hardware and applications that went through a firewall. That is the environment the legacy network security technology was based on. Over time there have been a number of transitions that have put more stress on security for an organization. Users are becoming much more mobile not only with regard to devices used, but also location; they may be inside one minute, then in another environment, and later in Starbucks. There has also been a transition on the data center side relative to how workloads and services are deployed shifting from a static environment with lots of time to think about time to set up new services to one that is very dynamic with workloads constantly spun up and down. Additionally, workloads can end up in infrastructure the security team isn't responsible for and doesn't have control over. There may be no ability to control anything in the infrastructure or the ability to deploy any protections as the user moves to the public cloud and SaaS applications. At each step there is a little less responsibility and control over the infrastructure, but the security team is still responsible for the user and data. Security companies need to cover this problem space so customers can take advantage of these transitions while managing risk and having necessary visibility and control in these environments.

Palo Alto started in the firewall at the perimeter of the network, or in the data center or for internal segmentation getting understanding, visibility and control but has moved beyond that. Solutions for mobile workers allow for ability to secure regardless of location. When mobile workers leave the institutional location and go to Starbucks or home, or an airport, it is important to still have all of the same security capabilities whether that is for URL filtering, prevention of malware downloads, application control to prevent peer to peer usage, etc. It is important to be able to do that consistently regardless of which network they happen to be using at that time. Global Protect is the infrastructure that allows Palo Alto Networks not be tied to a physical perimeter but to have a logical perimeter around the assets they are trying to protect and not to lose visibility when users go into someone else's domain.

"Traps" is Palo Alto Network's advanced endpoint protection product. It allows them to provide the next generation endpoint protection capability as it relates to antivirus and exploit prevention. Traps is an antivirus replacement and extension to really cover and do a much better job of preventing endpoints from getting breached and being used as a jump point into further activity inside the environment.

Palo Alto Networks collects a lot of interesting data and then leverages that data for threat analysis and threat hunting and really understanding the context around activities happening in the network. The goal is being able to detect and prevent malicious activity based on that data. The reason for making sure they are in all these places is to make sure they have the best opportunity to break the attack lifecycle and prevent the attacker from being successful. Whatever it might

be, whether a ransomware attack, or wanting to get to a random endpoint and encrypt it to collect on bitcoin, or trying to get into something to encrypt the file server infrastructure or trying to steal data. There are a series of steps required for attacks to be successful.

The first step in any attack sequence is for the attacker to get inside somehow, by leveraging a vulnerability that is network exploitable to get inside and attack a vulnerable endpoint inside they environment. Obviously, there is an opportunity to prevent that attack traffic even getting to that endpoint: IPS signatures to block on attacks and URL categorizations to make sure watering holes, phishing sites, malware domains, and so forth can't be accessed. There is an initial opportunity at that first step to prevent the infiltration. The second attack step after getting inside is to get content to the endpoint. The attacker typically uses two techniques: leverage a vulnerability exploit to get the machine to do something else, like download malware or get the browser to download some secondary payload which might be malware. This again provides the opportunity to do URL filtering, blocking malware sites and have the firewall controlling what kinds of traffic is allowed by application or by user. There is also network antivirus capability to prevent known malware from coming across the network as well. When malware gets down to the endpoint, there is another possibility, preventing the malware from executing which is the traditional domain of antivirus products.

Once the machine is compromised, there will be attempts to leverage control from a remote location, called "command and control" and there is an opportunity to prevent that. Application control looks at whether to allow use of Twitter, Facebook, or even DNS lookups which can be command and control mechanisms. Once the attacker is inside the network, if they are not on the target they will try to move laterally, to something with more privileges or more valuable assets. There again, is an opportunity to control the traffic flow inside the data center. Finally, the attacker's end goal is to get the data out which provides another opportunity to control that flow.

In the platform Palo Alto Network has tried to put together all of the components necessary to have the best possible chance at being effective in blocking the chain. If they were only at the firewall, a number of steps would not be possible, and there would be missed opportunities. All of the capability gives the highest possible probability of breaking the chain at some point. If there are eight different opportunities to block and each is 80% likely to succeed, there is a very high probability of success at breaking the chain of attack. The attacker on the other hand needs to be 100% successful at each step to be successful.

Palo Alto can compare URLs to known phishing sites to allow for blocking. They also proactively harvest links from emails that look suspicious and visit them in a WildFire sandbox for analysis to see if they are doing something inappropriate. They have a set of heuristics and behavior analytics used on new phishing sites

not seen before to characterize and categorize them once they are identified. Additionally, Palo Alto Networks can provide the ability to block the use of internal credentials in a public website through blocking for particular applications, like Facebook, or not allowing anything on a public site, or only allowing credentials to be used on the institution's site. They have technologies for preventing a phish for credentials. They also have a product called Aperture to inspect SaaS applications: Office365, email, or any sanctioned application. Aperture inspects and analyzes what is inside and if there is malware inside an email it can be quarantined, or the system can just alert you. Aperture uses the SaaS API to monitor and prevent malicious activity. The Aperture engine also has the ability to keep track of sensitive information: social security numbers, credit card information, PII, legal documents, code names, etc. and the firewall has data exfiltration to not allow that kind of data to go into the cloud, or to let it go through and have Aperture quarantine it.

Jeff cautioned that as a "man in the middle" solution, there might be political issues at educational institutions with breaking encryption to inspect traffic. Palo Alto Networks acknowledged that could be a concern, but it could be policy driven instead by blocking all malware categories, or decrypting uncategorized websites in China, or other ways to scope the decryption to very specific slices. There is full control to set up those kinds of rules and policies.

In summary Palo Alto is trying to bring together all of the pieces in a very automated, integrated fashion. They want the best visibility and ability to manage risk. What was formerly the perimeter is no longer the perimeter. Everything needs to be extensible: public cloud, on premise, and off premise. Total visibility is important, as is the ability to correlate across vectors and being able to correlate that data in a way that provides automated outcomes. Historically, security was focused on a "detect and remediate" model which was complex and tended to be in silos. Now with integration and automation Palo Alto is able to simplify and automate outcomes.

The goal is to provide predictable performance with all of the services enabled. When building Next Gen onto an existing legacy product there can be issues with service degradation, not being sure how long the product is going to last, and what the return on investment will be. On the other hand, Palo Alto was built with the native integration in mind which allows for a very consistent experience regardless of the services enabled and a consistent user experience across various types of Palo Alto products.

The Palo Alto Networks Next Gen firewall was demonstrated to show the granularity of information available. When logged into the dashboard it is possible to see very general information about the device logged into, about the appliance, and information about system resources.

The goal of the Palo Alto security platform is to safely enable applications for users or a user group but also to ensure that the content delivered over those applications is secure. This goal fits with three core technologies covered within the Palo Alto Next Gen Firewall: App ID, User ID, and Content ID. App ID looks at the issue of how to safely enable applications. The Next Gen Firewall is built on the concept of being able to identify all applications regardless of port or protocol. The Application Command Center (ACC) is the basis of App ID. It has sub tabs for network activity, threat activity, blocked activity, etc. All are customizable and a number of widgets can be added based on what is desired for the environment. The goal is to safely enable applications and the Application Usage Widget allows a view of information about the network based on how many bytes transferred over the last hour. Each element can be clicked to look at file sharing activity, rapid share, etc. User activity can be viewed, as can rule activity.

User ID is used to leverage and tie the firewall into the existing directory structure with Active Directory, CIS Log, or even SML API. It pulls in user identification information about who is leveraging different applications. Typically on firewalls, it is possible to see source, destination, and some session information, but details aren't really visible into what the user is actually doing. However, the ACC gives an overall, 30,000 foot view of the environment. A lot of institutions put the view on a big screen and refresh it every fifteen minutes to keep perspective on what is happening on the network. When a closer look is taken into what the user is doing from an application perspective, it is possible to look at the type of application being used on a scale of one to five, where one is not at all risky and five is very risky. These are customizable based on acceptable use policies for your organization, and risk level is determined by characteristics of the application, for example, if it is prone to malware, misuse, etc.

The demonstration drilled down into detail on the application, the user, and the content accessed on the network. Content ID looks at how to ensure that content being delivered is safe, and is broken into known and unknown threats. Known threats can be identified using a vulnerability protection profile and IPS, antivirus, or anti-spyware and DNS signature. Unknown threats can be identified in as little as five minutes by analyzing files with a service called WildFire which takes an unknown file and makes it known by detonating it in a known environment.

After identifying zero day malicious exploits, additional details and context are gathered to get actionable data. The WildFire event and details are passed to the Global Threat Intelligence cloud to be shared as actionable data. WildFire does a static and dynamic analysis by detonating the exploit on a virtual machine running XP and another running Windows7 to analyze behavior including what it modified, what the file activity was, etc. That information can be downloaded as a pdf to share with others. Global Threat Intelligence provides protection to

institutions within five minutes of being attacked. Additionally, every other subscriber will also get protections against that attack within five minutes.

A common challenging area for higher education institutions is URLs because they have to allow everything with open access policies, which can make it difficult to block threats. Often URL filtering is being leveraged as a standalone disparate point product, or is not offered at all. Palo Alto Networks has URL filtering natively integrated into the firewall which provides added benefits to the institution. Protections are provided every five minutes and include more information: not only "this file is bad," but also antivirus signature, DNS queries and virus signatures, exploits it is trying to leverage and IPS signatures, and URLs it is connecting to. Every five minutes URLs are being updated with respect to malware, phishing, etc. Additionally, specific to higher education is an unknown category labeled .xyz instead of .com that can often be malicious. Attackers are gambling on getting around URL filters since higher education is going to want to allow access, but having URL filtering native in the firewall allows colleges to take additional actions. They can disallow file downloads from that category or a variety of different activities. Native integration allows for quick action which is especially helpful in the higher education environment where one person is often managing multiple environments and gathering context and details for reporting is important.

The firewall can use a multi-faceted approach to identify and block proxy sites via URL filter, by application filter whether through signature or heuristics, or by category. Additionally, any new application released peer to peer is automatically added to that group and automatically added to the blocking policy. There is also an external dynamic list with all of the IP addresses which are automatically updated in the policy

Palo Alto Networks encouraged colleges to contact them for a non-intrusive proof of concept. They can do an installation behind the college's current security infrastructure to monitor the environment and produce a report on what the current structure is missing.

The Palo Alto Networks team will contact Tim about making a connection with the Foundation for CCC, which does system negotiation and contracting.

Next Meeting:

The next SAC meeting will be on May 25, 2017 at 1:30pm.

Adjournment:

The meeting was adjourned at 3:10 pm.