Constellations
Podcast

Special Release – Cyber, Satellite Security and the Space ISAC Vulnerabilities Lab

Speakers: Erin Miller, Executive Director and Ernest Campos, Co-chair of the Space Innovations Test Bed, Space ISAC – 17 minutes

John Gilroy: Welcome to Constellations, the podcast from Kratos. My name is John Gilroy and I'll be your moderator. The commercial space industry is facing an onslaught of cyber attacks and other threats, but what are the resources available for our industry to adequately defend itself? Today we will talk about the Cyber Vulnerabilities Lab, or CVL. It is one of the ways the Space Information Sharing and Analysis Center, or Space ISAC, is enabling the industry to benefit from a resource that can help. Our guests today are Erin Miller, Executive Director at the Space ISAC, and Ernest Campos, co-chair of the Space Innovations Test Bed for Space ISAC and Senior Executive for Space Programs at American Systems Corporation. Okay, Erin, we're going to start off with you. I talked about Space ISAC. What is the Space ISAC's Vulnerabilities Lab? What is its mission? A bunch of people in white coats or what is this lab all about?

Erin Miller: John, well, the lab is white, but there's no one with white coats on. So what is the Cyber Vulnerability Lab? I should tell you also what is Space ISAC. We are an information sharing and analysis center. We share information across the global space community. The whole reason why we exist is to raise the overall security posture for global space. Now, in order to do that, we knew we had to have a lab. So we have a Cyber Vulnerabilities Lab that focuses on doing hardware and software testing in an unclassified environment, and it gives the space community access to a trusted location so that they can conduct these tests. Now, what we expect is that companies are familiar with the process of doing hardware and software testing. They've probably done it a few times related to government systems. These are typically tests that happen in a classified forum. But this environment brings the whole community together, over 100 Space ISAC members, to have access and express their interest in prioritizing certain types of testing to disclose these vulnerabilities in a timely manner.

John Gilroy: Erin, the last time we spoke, you certainly didn't have 100 members. It sounds like this has increased like crazy the last few years. So when you initially started the Space ISAC, does this lab, does it fit with the rest of Space ISAC's purpose?

Erin Miller: It absolutely does. The watch center is the first thing that we opened to track the adversary from ground to space. We probably talked a lot about that last time. That's our operational mission. We have analysts in that watch center. This is an extension of the mission, always part of the vision, but we've got it in a phase right now where we've got companies who are looking through their portfolio of tests, and they're proposing them to the lab so that we can have a very fervent, exciting environment here where companies are actively bringing a capability to the lab.

It's interesting because it's not the ISAC staff. Space ISAC staff doesn't do this testing. It's actually a commercial company that's doing the test. They're doing early market testing, a different kind of testing, by bringing it to the lab environment and demonstrating to the community that this is needed, because they have that active feedback loop coming from the community. These are all community members that are trusted, MOU or NDA partners or members of the Space ISAC. So it's a very controlled environment here.

John Gilroy: Back in the days of Seinfeld, they had an episode that talked about naming names, and it was kind of funny. So I'm going to ask you to name names here, Erin. We talked about 100 members. Who are the industry players participating and how can other people in the industry get involved?

Erin Miller: Well, I can't name 100 companies off the top of my head.

John Gilroy: That'd be pretty boring.

Erin Miller: Yes. The industry players are all sorts of different companies, small, medium, larges. They're the ones out there who they have the highly reputable names, like the Lockheeds and the Northrops and the Kratos. There's also companies that are super small that you've never heard of, like Dark Sky Technology is one of the co-chairs of our Software Bill of Materials Task force, and NetRise, another active member in the software testing arena. These companies are making a name for themselves actually within this trusted community because we established a task force that would let them get involved and showcase their test. The goal is actually to use the task force to mature the understanding of the need that they fulfill so we can work towards a more operational model. And then we just do repeated testing in the lab and we disclose those vulnerabilities. I think that's something that Ernie could talk about quite a bit.

John Gilroy: Well, Ernie, he's part of the... I just asked the question. He's part of the answer. I guess he's one of the industry players who's participating. So Ernie, can you give us an example of how you test vulnerabilities? Can you maybe walk us through a scenario? Is there a sandbox or a red team or how do you test a vulnerability?

Ernest Campos: That's a great question. The process for testing vulnerabilities usually follows very defined directions, instruction, procedures, because we want to ensure that the proper steps are being followed to gain the most accurate results possible. Processes often include studying the effects of vulnerabilities on similar or like systems in other environments and observing what those experiences included, identifying what are called or known as signatures. When we can take those same vulnerabilities and apply them to space related assets, we can either anticipate expected results and confirm that we identify them, or we can document unexpected results that could create new signatures for other systems, space related or otherwise. But the processes usually follow use cases that are developed to ensure that step-by-step processing is followed. It's much like science. It's theory until it's proven over and over again. We like to ensure that the experiences that we are observing are very scientific in nature, and gives us a better opportunity to develop response methods to address those vulnerabilities.

John Gilroy: When people make observations, sometimes they're pretty boring and sometimes exciting things. I guess an astronomer might see a star exploding out there. So I'll ask you, have you found anything interesting that maybe you can share?

Ernest Campos: I have. There have been occasions where we have simulated disruptions in signals. As an example, radio frequency signals, which are often transmitted from satellites, back down either space to space, asset to asset, or space to ground. We've been able to not only monitor the transmissions, but also inject disruptions in those signals that emulate the types of disruptions that other individuals with less than wholesome intentions, I'll phrase it like that, the same methods that they might use. We're able to observe the types of impacts that those disruptions have so that we can document, learn, and train from those. And then we can even tweak the dials a little bit to identify what certain changes in those applications of interruptions might look like.

I'll also mention that when it comes to the testing processes that we're utilizing within the Cyber Vulnerability Lab that we're also adopting certain expectations and methods utilized by other ISACs governing other industries. Those are processes known as vulnerability equities processes, which not only ensure that there is equivalent forms of detecting vulnerabilities, but equivalent forms of disclosing them among ISACs as well.

John Gilroy: Ernie, you certainly are professional. Because I spoke to many people from the DOD, and they don't usually use the phrase less than wholesome. They use stronger language than that. I was like, wow, this Ernie, he's coached up. He knows the exact right phrase. I'm going to try that and see if they start laughing at me. Less than wholesome. So Ernie, are there plans for the CVL to host FlatSat or satellite software to simulate the space segment?

Ernest Campos: There certainly are collaborative efforts with other organizations who have already or simultaneously attempting to implement that same capability themselves. It can be very expensive to emulate space based assets, even in a flat format. So anytime we're able to share that type of test environment, it's a good collaborative effort.

One such collaborative effort we're working on is with United States Space Force, their Space Systems Command space domain awareness tools, applications, and process laboratory, also based here in Colorado Springs. That is an organization and a laboratory that seeks to provide solutions to known space related problems. We are attempting to apply the cybersecurity layer to their efforts through our collaborative efforts. If we're able to collectively develop a FlatSat environment where we can test those types of impacts in real time on site, that would be a wonderful gained ability for both of these organizations and others as well.

John Gilroy: So Ernie, is the concept of a digital twin part of this discussion here?

Ernest Campos: It is. It's not always applicable in every circumstance, but it is gaining its use and viability for these types of testing environments. It accelerates the ability to test, it accelerates the ability to recover from testing or from unexpected activities, and it also ensures that resiliency is built in to any lab's environment for their ability to always be ready and available for any type of test scenario that comes along. Right now, we have the luxury of testing without certain urgencies, but we envision a day where urgency will be a critical factor in our ability to test and test quickly.

John Gilroy: Ernie, I live in the Washington D.C. area. I've got friends in the military, ex-military. One of them used to work in red team and he did a lot of interesting things. So let's go back to this red team here. How will the CVL conduct red team activities and what are some of the pilot projects?

Ernest Campos: The ability to perform red team on live assets is always a preferred scenario. However, when we're talking about live assets that are performing functions in space, that's a more challenging approach. So our efforts to introduce red team capabilities will come through model and simulation capabilities. The ability to take actual assets, satellites or otherwise in space, with a digital representation, fully functional, made available on consoles where we can throw whatever we want added in terms of a vulnerability attack or attempt to infiltrate, and observe the results. Again, turn the dials to change the attack, change the results, learn the most optimum path to success towards protecting those space assets, all in the digital environment where you can press the reset button and start all over again. That is a very cost-effective method, that is a very low-risk method, and it does not disturb the actual satellites operational in space.

John Gilroy: Now, Ernie, I think there's an ethical component of this discussion today. So my question is, has the Space ISAC established rules that participants in CVL events must follow, which include the responsible public disclosure of any vulnerability? Touchy subject, isn't it?

Ernest Campos: It is. It is a touchy subject. But that's what's unique about Space ISAC and ISACs in general, is that their inherent disclosure of information and findings and the sharing of that information among other industry partners. For the CVL, yes, governance has been established through committees and charters and policies and procedures, which all dictate the boundaries of operation for any project or any endeavor that enters into the CVL. We're on common ground, we accept the rules, we abide by those, and we do it for the greater good of all the other member organizations functioning within the CVL.

John Gilroy: When I introduced this discussion today, I talked about the onslaught of attacks. Almost sounds like a military term, onslaught. But it seems that, given the increased focus on satellite security from events like Hackasac and the availability of tools like the satellite hacking cyberdeck, has the Space ISAC observed a rise in the number of threats or sophistication of attacks against satellites?

Erin Miller: John, the response that we're seeing from the industry to address the attacks against space systems is incredibly strong. That's why we have over 100 members and we have a growing global community addressing these issues. So it's led to an even broader conversation now. The Cyber Vulnerability Lab started as just a lab, and then it evolved to a conversation about building a network, basically a network of labs that would address the variety of different types of vulnerabilities that are in space systems.

What we're seeing is there's a priority across government, industry, and the global community to do a lot more testing in advance and create flight proven capabilities before deployment. These capabilities are not always as well known. Sometimes there's labs and test beds and proving grounds that sit there that are underutilized that could be used for this mission. This is where we see things that are going to address the number of attacks against space systems, and really just the overall attacks against critical infrastructure. We need to do more testing in advance and have more readily available accessible resources that operate in this same network of governance structure, and are willing to share the vulnerabilities as they're discovered in a high trust environment.

John Gilroy: Erin, let's take this up to 20,000 feet here. So your lab, we've been talking about this. So how does this lab contribute to the overall field of cybersecurity and space technology?

Erin Miller: We are using the lab to protect space assets. Truly in the purest definition of what the lab does is it detects vulnerabilities and anomalies. I think that we're still in the cultural transformation stage of this because to overall protect the field better of space and cybersecurity, we need more continuous training, like a space ISO course would be pretty helpful. For those who have a cybersecurity background, you'll know exactly what ISO is. Add space to that, and now you have people who are more well prepared to handle these circumstances where we have cyber attacks against space systems.

But then the lab itself doing responsible disclosure has also led to more conversations where companies are coming to us who are not even members of this Space ISAC who are conducting this act of responsible disclosure. The security researcher community, they reach out to us occasionally and we receive that information, the trusted community, and then now they become a trusted partner if they desire to be one. So we're overall shifting the mindset so that we can have more transparency and operate in a more proactive manner because of this lab.

John Gilroy: Erin and Ernie, you've really given the listeners a real good handle on the whole concept of security and responsibility with handling some of the ethical dilemmas in finding malicious actors, or maybe some people who have less than wholesome intent. I'd like to thank our guests, Erin Miller, Executive Director at the Space ISAC, and Ernest Campos, Senior Account Executive at American Systems Corporation. Thank you.

Erin Miller: Thank you.

Ernest Campos: Thank you.