Sayısal Mühendislik ile Uzayda Siber Güvenlik Tesisi

Gelecekteki başarı için beş anahtar unsur.

BRIAN PATE tarafından 1 Aralık 2022 tarihinde SIGNAL medyada yayınlanmıştır.

- 

Yer istasyonları, uydu altyapılarında önemli bir rol oynamaktadır. Bunlar sadece uydulara komuta ve kontrol sağlamakla kalmıyor, aynı zamanda uydu gruplarını internetin karasal omurgasına bağlıyorlar. (Kaynak: vchal/Shutterstock)

Sayısal mühendislik ve siber güvenlik araştırmaları geleneksel olarak tamamen farklı alanlar olarak ele alınmıştır. Bu iki uygulama, teknik evrenin farklı alanlarında, farklı sözlükler ve teknik özelliklere sahip olarak ortaya çıkmıştır. İki uygulama arasında köprü kurmak, uzay sistemleri de dahil olmak üzere siber-fiziksel sistemlerdeki güvenlik açıklarının tanımlanmasını ve düzeltilmesini önemli ölçüde iyileştirecek ve hızlandıracaktır. Bunları bir araya getirmek maliyetleri düşürecek, geliştirme hızını artıracak ve hayati önemde uzay birimlerinin üretim ve fırlatmadan yörüngedeki çalışmalarına kadar yaşam döngüleri boyunca güvenliğini artıracaktır.

Endüstriyel açıdan gelecekteki başarı için birkaç soru bir arada düşünülmelidir:

Siber güvenlik araştırma amaçları için benzetim ortamı yeterli midir?

Benzetim ortamları ve sayısal ikizler, geleneksel güvenlik açığı araştırması ve tersine mühendislik (Vulnerability Research and Reverse Engineering-VR/RE) uygulamalarını nasıl artırabilir?

Bu ortamda üretilen veriler, siber güvenlik araştırma hedeflerini desteklemek için yapay zeka/makine öğrenimi modellerini eğitmek için kullanılabilir mi?

Bu sorulardan, siber güvenlik araştırması için sayısal mühendisliğin kullanılmasına ilişkin tanımlanabilir beş önemli husus vardır. Bu iç görüler, sayısal mühendisliğin VR/RE kapsamındaki rolünü daha da güçlendirmek için gelecekteki iyileştirmeleri içermektedir.

Sayısal mühendisliğin önemi ve siber güvenlik araştırmalarının rolü

Sayısal mühendislik sayesinde, Modelleme ve Simülasyon (M&S) ürün geliştirme yaşam döngüsüne entegre edilir. Geliştirme ve testlerin çalışma ortamları, pahalı donanım bileşenleri veya oldukça karmaşık senaryolar gibi olağandışı durumlar içerilen ürünler için, sayısal mühendislik kanıtlanmış bir risk azaltma uygulamasıdır. Verimliliğin ve performansın arttırılma ihtiyacından doğan sayısal mühendislik, endüstrinin yeni ürün ve yetenekler tasarlama, geliştirme ve sürdürme şeklini değiştirebilir.

"Sayısal mühendislik" terimi genellikle yanlış anlaşılmaktadır, endüstri çapında benimsenmiş bir tanımdan yoksundur ve çoğunlukla etkisiz bir şekilde uygulanmaktadır. Bu engellerin üstesinden gelmek için, sağlam bir sayısal mühendislik yaklaşımının aşağıdaki temel ilkelerine uyulmalıdır:

Tek Doğruluk Kaynağı- Birçok alt sistem içeren karmaşık bir sistemi modellerken (bazen düğümler veya örnekler olarak anılır), mevcut ve üretilen durum verilerini düğümler arasında paylaşma yeteneği, sistem benzetiminin tek bir doğruluk kaynağı içinde çalışmasını sağlar. Bu, sistem modelinin ve ortaya çıkan benzetimin doğası gereği daha sağlam ve güvenilir olduğu anlamına gelir.

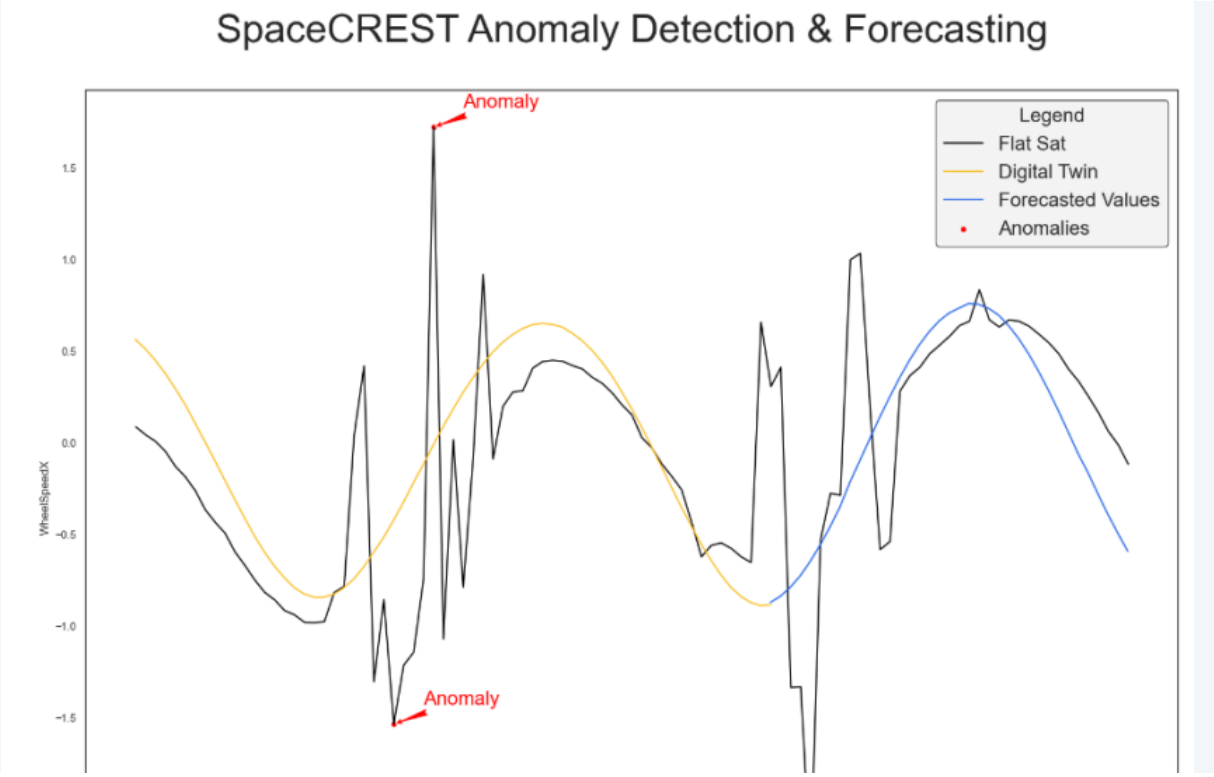
Sayısal İkiz Eserler- Mühendisler genellikle yaşam döngüleri boyunca modellere yinelemeli olarak aslına uygunluk katarlar; bu modeller, uygun şekilde tasarlandıklarında kolayca işletim sisteminin sayısal ikizlerine dönüştürülebilir. Sayısal ikizler, anormallik tespiti ve çözümü, tasarım güncellemeleri ve genel blok tasarım yükseltmeleri dahil olmak üzere birçok farklı amaca hizmet eder.

Bu ilkeler, sayısal mühendislik mükemmelliği ve güvenilirliği için ortak bir standart oluşturur.

Siber güvenlik açığı araştırması ve tersine mühendislik (VR/RE), kod analizi tekniklerini kullanarak elektronik donanım, ürün yazılımı ve yazılımdaki zayıflıkların belirlenmesi uygulamasıdır. Tersine mühendislik, bir sistemin veya uygulamanın onu bileşen parçalarına ayırarak nasıl çalıştığını anlamaya çalışır ve ardından nesnenin amaçlanan işlevini yerine getirmek için her bir parçanın birlikte nasıl çalıştığını yeniden oluşturur. Bir VR/RE araştırmacısı, fiziksel özellikleri belirlenmesi süreçlerini (donanım/firmware için), kod çıkarma ve statik ve dinamik kod analizi dahil olmak üzere çeşitli araçlar ve yöntemler kullanır.

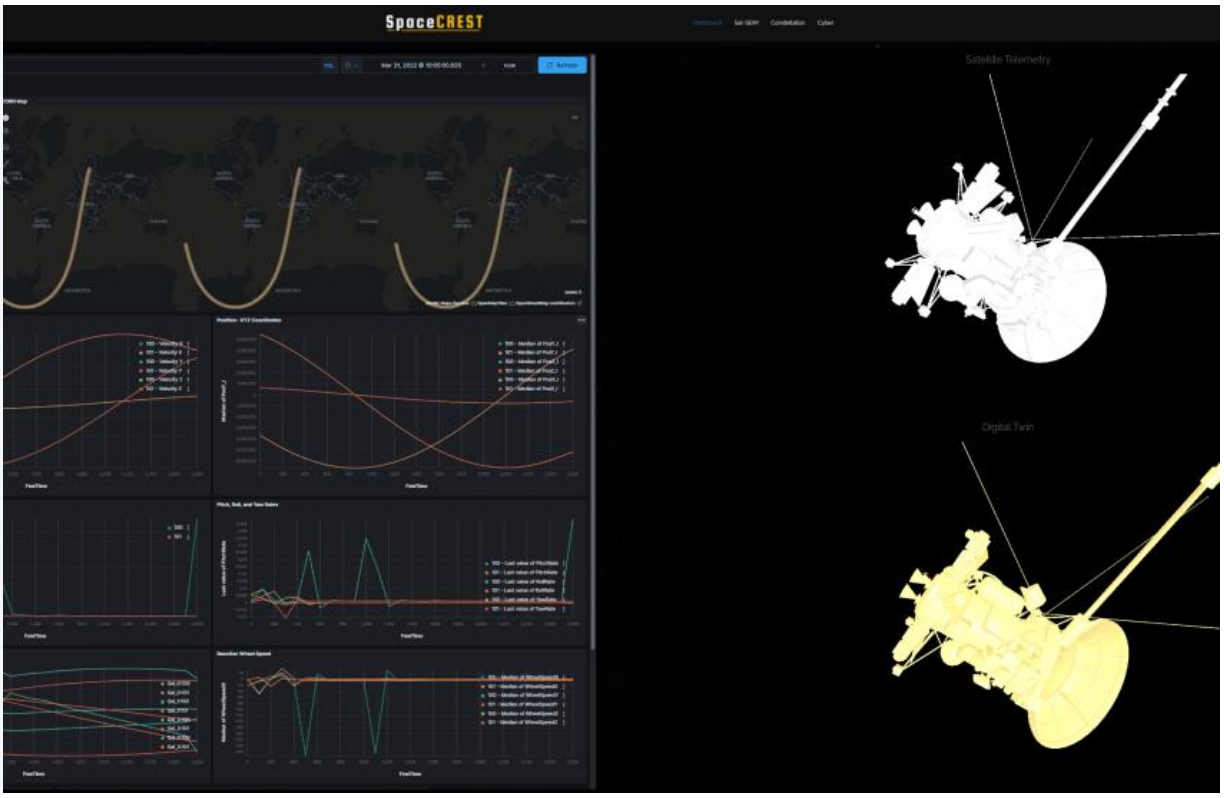
VR/RE, zayıflıkların düzeltilmesi veya diğer basitleştirmeler yoluyla sistemleri istismara karşı güçlendirmek için kullanılır. VR/RE geleneksel olarak kod analiz araçlarıyla zenginleştirilmiş elle yapılan işlemlere dayanır. Kodun son derece teknik doğasına rağmen, sıkıcı veri incelemesini, titiz dokümantasyonu, entelektüel merakı ve zor kazanılmış sezgiyi ödüllendiren uzmanlaşmış bir alandır.

Uzay ekonomisindeki patlama ve Savunma ve Uzay Kuvvetleri Bakanlığı'nın “Sayısal Mühendisliği” benimseme yönündeki baskısı ile siber güvenliği iyileştirmek için sayısal ortamın avantajlarından yararlanmak uzay sektörü, savunma sanayi ve genel olarak ulusal güvenliğe büyük faydalar sağlayacaktır.



Bu grafik, sayısal ikiz taban çizgisi ve tahmine paralel olarak anormal uydu bileşeni davranışının tanımlanmasını ve etiketlenmesini göstermektedir. (Kaynak: BigBear.ai)

Dünya Ekonomik Forumu'na göre, 2020 itibariyle dünyanın yörüngesinde 2.665 uydu dönüyor. Planlanan düşük Dünya yörüngesindeki takım uydu gruplarının bir sonucu olarak, bu sayının on yılın sonunda 100.000 uyduya çıkması bekleniyor. (Kaynak: Vadim Sadovski/Shutterstock)



Kibana tabanlı görselleştirme, saldırı altındaki bir benzetime paralel olarak çalışan temel bir sayısal ikizi karşılaştırarak durumsal farkındalık ve bağlamsal anlayış sağlar. (Kaynak: BigBear.ai)

Dikkate alınması gereken beş temel konu:

1. Modelin genişletilebilirliği. Tek bir "iyi" model veya benzetim faydalı olabilirken, araştırma hedeflerine ulaşmak için gerekli olan öğeleri ekleme, çıkarma ve iyileştirme yeteneği tercih edilmelidir. Modellere, bileşenlere, sistemlere ve üçüncü taraf yazılım entegrasyonuna izin veren genişletilebilir bir çerçeve, sayısal mühendisliği gerçek bir İsviçre çakısına dönüştürecektir.

Modelleme ortamına gelişmiş bir programlama arabirimi (Advance Programing Interface-API) güdümlü yaklaşım, döngü içinde donanım ve döngü içinde yazılım yetenekleriyle birleştiğinde, sayısal mühendislik ortamında esneklik yaratacaktır. Ayrıca, sistem çapında etki değerlendirmelerini destekleyen heterojen bir modelleme ortamı oluşturmak için "yeterince iyi" öğeler oluşturma ve bunları yüksek doğruluklu model öğeleriyle eşleştirme yeteneği de verir. Gelişmiş API'ler, herhangi bir donanım bileşeninin veya yazılım uygulamasının hızlı şekilde entegrasyonunu sağlar. Alt sistemlerin, sistemlerin ve/veya tüm bölümlerin mimarinin geri kalanı üzerinde çok az veya hiç etkisi olmadan verimli entegrasyonuna izin veren yapılandırılabilir bir soyutlama katmanı sağlarlar.

Açık bir sistem mimarisi, araştırmacılara saldırı etkilerini değerlendirmek için daha fazla seçenek sunabilir. Örnek olarak, bir araştırma senaryosunda yer alacak benzetilmiş bir tepki çarkına[1] yönelik bir hizmet reddi (denial-of-service) saldırısının, uzay aracı benzetiminin diğer bileşenleri üzerindeki etkisini değerlendirebilir.

[1] Tepki Çarkı: Uzay aracı tarafından üç eksenli konum kontrolü için kullanılır ve roketler veya harici tork uygulayıcıları gerektirmez.

Araştırmacılar, hizmet reddi saldırısına dünya üzerindeki farklı bir noktayı işaret ederek tepki veren bir "döngü içinde yazılım" kamera modülü oluşturabilirler. Açık sistem mimarisi, araştırmacılara saldırı etkilerini değerlendirmek için daha fazla seçenek sunar. Bu işlevsellik aynı zamanda harici araştırma ekiplerinin fikirlerini veya araştırma hedeflerini aynı ortam içinde iş birliği için getirmelerini sağlar.

2. M&S Sisteminin Etkinleştirilmesi. Sayısal ortamı izleme, etkileşime girme, çalıştırma ve sürdürme yeteneği olmadan, hantal, yetersiz optimize edilmiş bir ekosistem haline gelebilir. M&S sistemini iyi hazırlanmış ve araçlarla donatılmış bir altyapıya düzgün bir şekilde uyarlamak, daha değerli iç görüler üretecektir.

Altyapı, etkileşimli araçları ve veri analizini tam olarak desteklemek için güçlü bir veri yakalama, depolama, analitik ve görselleştirme yetenekleri içermelidir. Birkaç tam yığın seçeneği bu altyapıyı sağlayabilir. Bunlardan biri, bu işlevleri desteklemek ve M&S sisteminin yerel kullanıcı arabirimini artırmak için Elastic'in ELK (Elasticsearch, Logstash ve Kibana) yığınını çalıştıran bir Nutanix bilgi işlem kümesidir.

Bilgi işlem kümesi, test edilen benzetimin klonlanması yoluyla sayısal ikizlemeyi desteklemelidir; bu, paralel çalışan benzetimlerin oluşturulmasını sağlar. Bu aynı zamanda yeniden oynatma ve Monte Carlo yöntemlerini destekler ve yapay zeka/makine öğrenimi araştırması için istatistiksel analiz ve model eğitimini desteklemek üzere verileri yakalar.

3. VR/RE sonuçlarının doğrudan model doğruluğu ile ilişkili olması. Benzetimi yapılan her sistem mükemmel bir model gerektirmese de karmaşıklık arttıkça sistemler arasındaki beklenmedik etkileşimlerin kaçınılmazlığı da artar. Anlamlı sonuçlar sağlamak için, benzetimin aslına uygunluğu, makul bir doğruluk sağlayacak şekilde düşünceli bir şekilde tasarlanmalı ve model eksiklikleri dikkate alınmalı ve gerektiğinde iyileştirilmelidir.

M&S dünyasında, tüm benzetimler eşit yaratılmamıştır. Fizik modelleri bir sistemin özelliklerini taklit eder ve sistem ilişkisi modelleri (model tabanlı sistem mühendisliği yazılımı gibi) sistemler arasındaki ilişkileri taklit eder, ancak sistemin protokol düzeyindeki davranışlarını tam olarak kopyalamaz. Karma uzay benzetim ortamında, bir bileşen bir uzay aracı elemanının fiziğini taklit edebilir, diğeri döngüdeki gerçek bir donanım elemanı olabilir ve tamamı sanallaştırılmış bir yer bölümüne bağlanabilir.

Bu nedenle, ortamın sınırlamalarını anlamak son derece önemlidir. Sistem genelinde tam protokol düzeyinde paket izlenebilirliği oluşturmak için, belirli güvenlik açığı sorularını yanıtlamak için tüm öğelerin yüksek doğrulukta protokol düzeyinde öykünmeler olması gerekir. Aslına uygun öykünülmüş bileşenlerden oluşan bir kitaplık geliştirildikçe, olası güvenlik açığı araştırmalarının derinliği zamanla artar. Bu sınırlamalarla bile, saldırı senaryolarını otomatikleştirme ve uzay aracı boyunca fiziksel etki yayılımını değerlendirme yeteneği paha biçilmezdir.

4. Temel güvenlik açığı araştırma ilkelerinin geçerliliği. Geleneksel güvenlik açığı araştırma ilkeleri geliştirildi, değiştirilmedi. Sayısal mühendisliğin entegrasyonu, endüstrinin denenmiş ve gerçek araç ve tekniklerini geçersiz kılmaz; bunun yerine, daha anlamlı ve verimli değer sağlamak için bu araçları uygulamanın yenilikçi yollarını sağlar.

Bir güvenlik açığı değerlendirme çerçevesi, sayısal mühendislik ortamındaki geleneksel VR/RE yöntemlerinden yararlanmalıdır. Bu yöntemler çoğu VR/RE uzmanına aşina olmalıdır: IDA Pro, Ghidra ve diğerleri gibi mevcut sınıfının en iyisi araçları kullanarak statik ve dinamik analiz. Çerçevenin sayısal mühendislik unsurunun bir odak noktası, benzetim yoluyla

davranış analizinin eklenmesidir. Bu, senaryoları hızlı bir şekilde oluşturma, komut dosyası oluşturma, otomatikleştirme ve izleme becerisini destekler ve istatistiksel ve makine öğrenimi karşılaştırmasını ve her bir benzetim çalışmasının analizini desteklemek için veri normalleştirme yöntemleri sağlar.

5. Gerçeği unutmayın. Gerçek dünya veri doğrulaması, sayısal mühendislik yaklaşımlarına dayanan bulgular ve kararlarda güven oluşturur. Benzetim ortamının gerçek çalışma ortamıyla eşleştiğinden emin olmak için sayısal modelleri kontrol etmek önemlidir. Bu, M&S sistemi tarafından üretilen sentetik verilerin makine öğrenimi analizine dayalı kurallar geliştirirken özellikle doğrudur. Bir uzay aracına yönelik bir saldırının göstergelerini ve uyarılarını sağlayabilen anormallik tespit modellerini geliştirmek için kullanılan sentetik veriler için, model ve veriler, gerçek dünyadaki temel verilerle karşılaştırılarak doğrulanmalıdır. Bu doğrulama süreci aynı zamanda model geliştirme için bir geri bildirim döngüsü oluşturarak sentetik verilerin kullanışlılığını ve doğruluğunu daha da artırır.

Sayısal mühendislik, siber güvenlik araştırmaları için parlak bir gelecek vaat ediyor

Siber güvenlik araştırması için sayısal mühendislik platformlarını kullanmak yalnızca mümkün olmakla kalmaz, aynı zamanda uygun maliyetlidir ve araştırmanın kalitesi, gerçek bir siber-fiziksel sistemin değerlendirilmesiyle eşittir. Bu sonuç, daha önce tanımlandığı gibi önemli uyarılarla birlikte gelir, ancak iki disiplin gelişmeye devam ettikçe, sayısal ortamları VR/RE amaçları için kullanmanın etkinliği yalnızca artacaktır. İki disiplinin sürekli entegrasyonunun daha güvenli uzay sistemlerine yol açacağı kesindir.

Brian Pate, BigBear.AI'de ABD Siber Uzay Komutanlığı, hizmet siber bileşenleri, İç Güvenlik Departmanı Siber Güvenlik ve Altyapı Güvenliği Ajansı ve siber uzay görevleri olan diğer ABD hükümet kuruluşlarına tam spektrumlu siber uzay hizmetleri ve çözümleri desteğine odaklanan Siber Operasyonlar İş Birimine liderlik etmektedir. Bu makaleye katkıda bulunan diğer kişiler arasında BigBear.AI'deki başlıca güvenlik açığı araştırmacıları olan Joe Davis ve Steven Durr ve Redwire Space'teki görev mimarları Alex Dunn ve Danielle Cleveland yer alıyor.

https://www.afcea.org/signal-media/cyber-edge/enabling-cybersecurity-space-digital-engineering