CHIPS THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE

Email

A new cyber-resilient approach for warfighting platforms

By Tracy Gregorio - January-March 2023

Our nation's critical warfare assets, such as Arleigh Burke class destroyers (DDGs) and the AEGIS Weapons System (AWS), are uniquely difficult to protect from cyberattacks. They are examples of large Systems of Systems (SoS) running multiple concurrent mission threads, presenting vast numbers of threat surfaces that include complex integrated systems, satellite communications links, sensor fusion platforms and many human/machine interfaces.

Commands need those systems to have the resilience to stay on mission no matter what type of cyberattack they are subject to. While existing defensive cyber capabilities adequately monitor for vulnerabilities, it's been difficult, if not impossible, to identify which cyber threats pose the greatest threat to mission effectiveness. The resilience challenge is difficult because commands need to simultaneously grapple with three factors:

1. **Their systems and subsystems continuously face multiple concurrent threats.** With vulnerability monitors flagging multiple threats, how should analysts prioritize which threats to focus on? Which could most impact their mission or missions? Analysts need to understand if and how those threats across information technology (IT) and operational technology (OT) systems might impact their ability to complete missions through denial of service, performance degradation or data loss.
2. **Cyber threat actors relentlessly create new exploits.** Threats come in at such a pace that it's unrealistic to evaluate all potential threats and vulnerabilities, to know which might succeed, and which could compromise mission capability. A single vulnerability in a critical component could render a unit useless, while multiple vulnerabilities in another subsystem might mean cyberattacks can disrupt a series of operations, while the ability to execute mission-critical operations remains in full force.
3. **Deployed platforms are not static.** Major platforms like the Arleigh Burke class DDG have useful lives across three decades or more, during which their IT and OT systems experience continuous spiral updates. A common byproduct of this, however, is that the platform drifts from its documented design baseline through poorly documented break/fix field workarounds, unplanned commercial-off-the-shelf (COTS) obsolescence refreshes and cumbersome configuration management processes.

There is, however, an approach suitable for optimizing cyber risks across the most sophisticated SoSs. Our engineering team has been working through a pair of Small Business Innovation Research (SBIR) programs to better protect parts of some of the Navy's most important

warfighting platforms and weapons system programs. These solutions involve four elements that can be readily extended to other platforms:

1. **Model the baseline.** The first step involves creating a digital twin of the complete SoS including every subsystem, interface, data flow and mission thread. Model based system engineering (MBSE) captures the architectural and functional characteristics of each and every system interface via a high-fidelity digital twin model. This enables all potential cyberattack surfaces to be captured via a disciplined and standardized engineering approach. These digital models represent the architecture and operational behaviors through Systems Modeling Language (SysML) diagrams spanning from the mission threads down to the IT and OT Configuration Item (CI) levels. Each digital twin is created to represent the real-world as-is state of the platform. Baseline management and change management changes can then be automated to deal with design volatility, rapid refresh/insertion rates and ensue commonality between platform variants.
2. **Connect intelligence repositories.** The next step in the approach is to cross-reference the digital twin against the latest threat intelligence databases. Automated processes are set up to ingest, aggregate and correlate threat data from open as well as classified sources and map those to the architecture. This optimizes use of the National Institute of Standards and Technology (NIST) and other threat/vulnerability frameworks, showing how vulnerabilities and attack vectors can impact operational and mission threads rather than the traditional focus on devices, networks or enclaves.
3. **Simulate mission risks.** With the MBSE model connected to threat databases, algorithms are created to simulate attacks, analyze mission impacts and probabilities, and rank mitigation strategies through defensible Objective Quality Evidence (OQE). This arms commands with the ability to drill down on platform and mission cyber risk and develop remediation recommendations ready for prioritizing, decision-making and approval. Over time, system architects can model and refine cybersecurity strength focused on mission, driving up critical system resiliency while lowering maintenance and sustainment costs.
4. **Monitor and control.** All this information is brought together and made usable through simple graphical dashboards. These enable analysts to use historical and trend analysis to act quickly to implement configuration changes, isolate known vulnerabilities and identify undiscovered attack vectors.

This approach is available as an approved Phase 3 SBIR program to help Program Executive Offices (PEOs) and field commands avoid seeing every vulnerability as equally urgent. It helps them prioritize fixes and allocate mitigation funding to align resources with the command's mission priorities.

Tracy Gregorio is a model-based systems engineering and security engineering solutions expert and provides contractor support to the Naval Sea Systems Command (NAVSEA).

TAGS: CISO: Cybersecurity, Cybersecurity, Strategy, Telecommunications