CYBERSECURITY FIRST

CECOM SEC leads Zero Trust implementation.

by Kevin Deegan

In an age when the U.S. government reinforces strategies to protect critical data from the exploitive actions of nation-state and non-nation-state attackers, the Army continually relies on top experts to implement new strategies. And in today's digital world, cyberattacks are becoming more sophisticated and widespread. To combat these threats, organizations must adopt Zero Trust (ZT) Architecture.

An Executive Order was signed in 2021 that calls for improved national security. Section three of the order detailed the need for ZT Architecture.

But what exactly does this mean, and how does it protect against cyberattacks? ZT is a modern approach to cybersecurity that operates on a simple but powerful principle: never trust, always verify. Unlike traditional security models that assume everything inside a network is safe, ZT assumes that threats can come from anywhere—inside or outside the network. Therefore, every user, device and application that tries to access your resources requires continuous verification.

The U.S. Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) supports the technical navigation of this ever-present cyber conflict. In early 2024, Farhat Shah, a cybersecurity expert, began spearheading the SEC's policy and procedure development for ZT cybersecurity.

LEVERAGE EXISTING SECURITY CONTROLS

Shah and her team led an initiative to integrate ZT principles into our existing systems. The SEC's goal in the initiative was to build upon the existing risk management framework (RMF—the security framework that systems must follow) controls. By leveraging existing controls, the team aimed

to create a ZT readiness profile and was successful in enhancing system security without duplicating efforts.

The focused approach of optimizing current configurations for ZT alignment allowed the team to make systems more resilient. Building upon the RMF ensured a smoother transition to ZT with minimized disruptions.

The transformative effort involves aligning current cybersecurity guidelines with more efficient, beefed-up ZT security measures. The SEC is referencing the Department of Defense (DOD) Zero Trust Overlay, a document published in June 2024, to meticulously map the Control Correlation Identifiers (CCIs). Mapping the CCIs makes the policy implementable and measurable.

"The Zero Trust framework is not a new piece of technology per se, nor a service that one can acquire and implement. In essence, it's a concept that, in simpler terms, is 'never trust, always verify,' " said Shah. "To holistically achieve Zero Trust, we're not coming up with anything new that the Army hasn't seen—we're building upon our current capabilities, and we are building Zero Trust in," she added.

The overarching aim of developing a ZT implementation policy baseline was to further bolster the Army's efforts in protecting critical data from the preying advances of nation-state and non-nation-state attackers and rogue hackers who intend to harm and disrupt U.S. interests across its cyber infrastructure and beyond. The new policy stands as another case of the Army's requirement to employ enhanced, sturdier countermeasures in the face of emerging, ever-changing cybersecurity threats. The first-of-its-kind effort seeks to aid the Army in maintaining constant vigilance of critical network resources while rigorously adapting its cyber posture to stay ahead of the game.

BUILD ON THE FOUNDATION

The SEC is using the DOD Zero Trust Security Control Overlay to map and implement changes to the current RMF. Mapping the new policy to the existing RMF is critical to upgrading the cyber posture.

A CLOSER LOOK

Long-term goals for SEC include incorporating ZT further into Army and DOD systems and developing workforce training programs around the organization's methodology. (Graphic by Kim Miller, CECOM SEC)

Unlike traditional security models that assume everything inside a network is safe, ZT assumes that threats can come from anywhere—inside or outside the network.

"It's not a tool, and it's not a one-time deal—[Zero Trust] is a concept that requires a careful implementation of policies, integration and continuous monitoring that provides the highest level of protection for assets and data," said Shah. "I think the biggest challenge is the cultural shift," she continued. "There is some change required in the way we do business in cybersecurity."

SEC's core focus remains on implementing ZT into the warfighter's practice while reducing the learning curve and improving cyber practices within the Army and DOD. In an increasingly hostile cyber environment, SEC will continue to prioritize ZT integration as it moves to bolster the Army's overall cybersecurity posture.

AI AND ML ACTIVITIES

Multi-agency collaboration will play a critical role in shaping cohesive ZT policies. SEC works closely with external stakeholders to ensure ZT efforts are aligned across different entities. Collaborations focus on shared information, best practices and insight into agency-tailored policies supporting a unified security posture; cooperation across organizations is essential.

Standardizing policy involves working with external stakeholders to establish consistent and effective ZT guidelines. Agencies must ensure that policies are complete and compliant with DOD standards . . . but they must also be practical. One critical focus is meeting the challenges of securing tactical systems, which often live in complex, demanding environments. By creating standardized policies, SEC's goal is to simplify compliance and enhance the overall security framework, making it easier for teams to adopt and implement ZT practices.

SEC is currently aligning the DOD ZT model with RMF controls with artificial intelligence (AI) and machine learning (ML) activities to enhance security outcomes for future systems with those capabilities. The alignments are critical because they ensure that ZT is fully incorporated into compliance processes related to AI/ML technologies that enable threat detection and automated responses. Bridging the gap between innovative security and traditional risk management empowers the DOD to stay ahead of evolving threats.

CONCLUSION

Whether running a small business, working in a large corporation or just worrying about personal cybersecurity, the ZT approach minimizes risks and enhances security. The ZT framework is a vigilant security guard for the digital world—one that never sleeps, never assumes and always ensures protection. By embracing ZT, organizations can avoid cyber threats and ensure the security of their data, systems and people.

For more information about SEC ZT efforts, contact Farhat Shah at ***farhat.shah4.civ@army.mil****.*

KEVIN DEEGAN provides contract support to the U.S. Army Communications-Electronics Command at Aberdeen Proving Ground, Maryland, as a strategic communications specialist. He holds a B.A. in journalism from Temple University and is certified as a Project Management Professional.

CONTRIBUTOR: *FARHAT SHAH is the cybersecurity expert for the Department of Defense.*