ATARC paloalto® NETWORKS

Powered by GovExec

Safeguarding Military Infrastructure and Frameworks: Opportunities and Challenges | West Mountains

Highlights from a Roundtable hosted by the Advanced Technology Academic Research Center (ATARC) in partnership with Palo Alto, December, 2024

In a recent roundtable, Federal experts discussed several pressing cybersecurity challenges facing the government and DoD today. The discussion focused on the challenges of protecting a widening perimeter, defending against AI threats, preparing for emerging quantum technology, and reframing the concept of cybersecurity risk to end users. Panelists closed the discussion by sharing prescriptive strategies to help safeguard military infrastructure and frameworks in this evolving landscape.

Defining the Perimeter

Panelists discussed the challenges with protecting the entire lifecycle of software development, noting that before cloud environments, the lines around network perimeters were clearly marked. Now, there are no defined boundaries or clear access points. The complexity of cybersecurity lies in the multitude of decisions that must made to not only determine access, permissions, and roles for anyone interacting within the amorphous network, but also defend the blurry boundaries from threats.

> **“Our perimeters aren't physical anymore. They're virtual.”**

Panelists agree that in 5 years there will no longer be a semblance of a perimeter, since most work is conducted through internet browsers. As such, agencies need to shift their cybersecurity postures to start cybersecurity chains at the information exchange boundary. A panelist referred to John Holland's book Signals and Boundaries to illustrate this concept, noting that moving forward, agencies should think of a cybersecurity boundary as a semi-permeable membrane where agencies can manipulate that permeability to allow different data types across.

There are tools and scanners to help identify vulnerabilities, but panelists note challenges with trusting software updates from vendors or third parties. There could potentially be vulnerabilities within the software supply chain that agencies are unaware of.

Challenges with Shared Infrastructures and Systems

Sharing infrastructure or systems with customers, markets, or stakeholders adds another layer of complexity to safeguarding government network perimeters. Sharing information is a component of many missions, but interacting with multiple agencies with different security postures while ensuring information is secure is increasingly complex. Ultimately, as one panelist noted, you can’t protect all information. What agencies can focus on is designing systems to be more resilient in the wake of a rapidly changing environment.

Encryption Verification of Hardware Devices

Panelists also discussed the challenges with securing devices and IoT in the context of securing a widening perimeter. A panelist noted the difficulty for the end user to verify whether devices are truly encrypted while out in the field. Although there are multiple layers of security and encryption on devices, panelists acknowledge that agencies cannot rely on the end user to ensure the security of a device. Another panelist shared that the industry is beginning to develop zero trust solutions on a SIM card to help bolster security in devices.

AI and Quantum Computing

Discussion continued with panelists sharing myriad challenges around rapidly evolving technology, especially AI and quantum. Panelists note that AI has significantly accelerated the threat landscape as adversaries rapidly began to adopt the technology after the emergence of open AI. Now, after a breach, adversaries can move laterally within a system in hours. Only a year ago, this type of lateral movement took weeks.

As such, current detection methods are no longer viable, yet most SOCs are designed around detection. Moreover, systems receiving data are not integrated with one another, which makes automation challenging. Pulling disparate systems onto a single, holistic platform is the key to continuously monitor threats.

Quantum computing is expected to magnify and exacerbate this problem. Industry is already working on full quantum crypto suites to better protect boundaries, data, and storage and help prevent future decryption attempts. Ultimately, the goal is to encrypt user traffic across the network. Although post quantum is likely years away, agencies should begin building systems for the future and not just for today's challenges.

> **"Post quantum is years out, but that doesn't mean we don't acknowledge it and do something about it now. Because if we wait, we're done. You can never get too comfortable with what you're doing."**

Some panelists at the roundtable are still very hesitant to apply AI to current systems, namely because there are proven AI hacking methods being employed that are poisoning data. Fixing an issue like data poisoning requires more than a re-install. It would require rebuilding and retraining an entirely new LLM model.

Panelists note that the potential for AI to support the work of engineers, for example, is great. However, panelists note that those using the AI must be able to make sense of and validate outputs within the context of the system. Panelists reiterated the critical importance of trusting data.

Panelists continued discussing the complex interplay between humans and machine, and the need to determine the appropriate role of humans in systems where many low-level decisions are automated. The challenge faced by agencies lies in identifying when these simple, automated decisions turn into complex situations with unpredictable effects. The panelist contends that humans must be positioned to handle these emergent effects since they can't be predicted by machines.

Panelists also mentioned physics infused machine learning, which is the next frontier in LLM models. There will be groundbreaking applications in blood analysis, genetics, and thermodynamics. AI and ML will be in all areas of critical infrastructure, so it's essential that agencies are able to measure the effectiveness and trust in the data of a machine learning system.

Reframing the Concept of Cybersecurity

A large portion of the roundtable discussion centered on the importance of reframing the concept of cybersecurity among the workforce. One panelist illustrated this by describing the secondary and tertiary effects of a cyber attack on a prescription medication supply chain. Laws aimed to prevent overdoses and illegal sales are in place to limit certain medication supplies to 30 days. However, supply chain disruptions caused by cyberattacks to

> **"The DoD mission is not just dependent upon what's inside the fence. There are many other entities outside the fence. It's only becoming more complex. The whack-a-mole approach doesn't work in the same way."**

insurance systems, for example, can leave patients without essential medications and lead to severe health consequences. The panelist highlighted the need for policy flexibility to help mitigate the risks associated with such unforeseen events. The ripple effects of cyber attacks also extend to response and recovery efforts. Panelists acknowledge that there has not been enough focus on the responsive recovery of attacks that may coincide with extenuating circumstances, such as extreme weather events.

People Culture

> **“What’s the biggest challenge? It's not the technical solutions. It's processes, people, and organizational acceptance of risk. It's funding models. It's finance.”**

Panelists discuss the challenges with building a more informed culture around technology, cybersecurity, and especially AI adoption. Panelists clearly see scenarios where end users implicitly trust AI outputs, without questioning the validity or quality of data. Panelists note that as AI use proliferates, it will become more important for the end user to accept responsibility for their mistakes that may affect cybersecurity. To begin shifting this culture, panelists recommend using incentives to ensure cybersecurity is an intrinsic component of everyday work.

Panelists also note a lack of situational awareness among leadership, where leaders too often are not aware of their cyber resilience status. This lack of awareness is impacting the quality of their decisions. Panelists acknowledge that cyber professionals are doing a poor job quantifying cyber risk to leaders, making it more challenging to set goals and allocate resources effectively. Having the ability to measure security can help agencies better understand their risk levels. Trusted data can help agencies better communicate risk to upper management.

> **“There are roadblocks, and the roadblocks go back to people.”**

One panelist highlighted the need for cyber professionals to better translate cybersecurity concepts into language that systems owners and procurement personnel can understand.

Safeguarding Solutions

> **“We can't do this alone. Zero trust isn't a product, it's a mindset. It's a continuous improvement process.”**

Panelists continued the discussion by exploring several key tenets of an effective safeguarding approach.

- **Collaboration among vendors** - effectively implementing a zero trust policy will likely require the collaboration of multiple vendors. Panelists highlight the challenge of transitioning user intent across different policy enforcement engines, which can lead to a dilution of the original policy’s intent. Industry cooperation is key to ensure the agency’s zero trust intent is enforced consistently and seamlessly throughout the system.

- **Automation** - Automation is necessary for rapid response to network threats. Reactions to threats must take hours or minutes, not days or weeks.

- **Leverage existing infrastructure** - Due to the high costs of building new infrastructure, it’s not feasible to completely overhaul existing IT infrastructure to comply with zero trust. Panelists recommend leveraging and integrating existing tools to create a secure platform.

- **Improve user experience** - Improving the user experience whenever possible is key to prevent users from finding security workarounds.

- **Conditional access** - Conditional access is vital to control network access based on context.

- **Browser and security** - Panelists contend that the browser is likely to become the first place of security and the point of ztna connection.

Final Thoughts

Panelists concluded the roundtable with a strong emphasis on the need for collaboration between industry and government to advance cybersecurity. They pointed to the importance of employing prescriptive zero trust solutions through a unified platform to effectively safeguard infrastructure and frameworks. Companies like Palo Alto Networks are actively working on integrating advanced protection measures, including IDS, IPS, DLP, IoT detection and response, URL filtering, sandboxing, DNS security, SaaS security, and more, into their platforms.

The discussion also underscored the need for ethical standards for vendors. These standards would help streamline secure product development and prevent a "race to the bottom" scenario driven by cost-cutting priorities, ensuring quality and security are not compromised.

Ultimately, the panelists agreed that fostering collaboration between government and industry is critical to accelerating the development and adoption of robust cybersecurity strategies. They highlighted the value of roundtables like this one in creating a shared brain trust, bringing together diverse skills and perspectives to address pressing challenges.

LEARN MORE AT: WWW.PALOALTONETWORKS.COM/