Wednesday, August 17, 2022
12:00 NOON – 12:20 PM
Leveraging Zero Trust and Strong Authentication Across Unified DoD Networks

Alex Antrim
Senior Solutions Engineer
Yubico

Abstract:
Defense Department IT professionals have practiced a defense-in-depth strategy for years relying upon a series of firewalls for fundamental security against predicted and known threats. However, in today's post COVID-19 world, the attack surface is changing as network access is moved away from traditional perimeter based security to cloud based security, making the former security strategy increasingly irrelevant as a way to protect networks, data, and intellectual property. That's especially true given the proliferation of privileged accounts that give users the ability to access sensitive data and applications, including ubiquitous devices, like smartphones and tablets, that allow access to Department of Defense (DoD) networks. Together, these avenues of access have one vulnerability in common: the username-and-password login process.

What's the single wall that's blocking nation states, rogue actors, and cyber criminals from hacking email accounts? The log-in screen, with potentially weak authentication methods that result in a vulnerable cyber defense strategy. Firewalls are no longer effectively serving that purpose. Instead, remote identity proofing, access management, and strong authentication are quickly becoming the new bulwark against cyberattacks. As the DoD moves to securely make data and resources available to service members and employees around the globe, the need for strong authentication that is device agnostic is crucial. Modern phishing-resistant authentication protocols must be employed by end users regardless of the device being used to access data and resources. This is accomplished by leveraging a multi-protocol external hardware authenticator, effectively bridging tried and tested PKI over to FIDO2, while still supporting legacy authentication on air-gapped networks. A unified network requires a strong foundation of identity and authentication in order to meet zero trust and securely provide data-centric resources to the warfighter. Strong authentication is required across all of the top use cases in the DoD: Bring Your Own Device (BYOD), privileged users and administrators, non-CAC eligible employees and dependents, and shared devices at the tactical edge. Each of these is supported by a multi-protocol, multi-factor, AAL3 hardware authenticator like the YubiKey.

This session will describe the value of modern authentication for and how multi-protocol authenticators can support a wide range of use cases for the DoD. You'll also hear how the confluence of world events and federal government directives enhanced the evaluation and piloting of CAC-alternative authenticators.