DEFENSE INNOVATION BOARD
Zero Trust Architecture (ZTA) Recommendations
Kurt DelBene, Milo Medin, Richard Murray

IMPLEMENTATION RECOMMENDATIONS

Based on existing Department of Defense (DoD) network vulnerabilities and future network requirements, the Defense Innovation Board (DIB) recommends that DoD begin moving toward a zero trust security architecture model for the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). While zero trust implementation will be an iterative process across various DoD networks, all DoD zero trust efforts should strive toward the following **network ecosystem end state**:

- Continue to use perimeter security around the network, but acknowledge that network breaches can and will occur.
- Operate under "least privilege access model," where network users by default do not have access to any applications or services in the network. Even if an unauthorized user breaks into the network, that user should not be able to access any sensitive data or services.
- Grant access at a granular level depending on the role of the user (with attributes including but not limited to organization, project, and clearance level). These attributes should be shared across DoD networks to enable efficient, targeted access management.
- Consistently leverage multi-factor authentication (MFA) to validate identity and access at the network perimeter and for each network resource.
- Monitor health of any devices plugging into DoD networks to block access for compromised devices and drive device configuration best practices.

To achieve these long term goals, the DIB has developed recommendations for near-term implementation. ZTA requires a holistic view of network security that ranges from DevSecOps to mission system software management,[1] but for the purposes of this paper the DIB has focused on authentication, authorization, and encryption methods for DoD. These recommendations are intended to serve as a common baseline for organizations to synchronize their zero trust efforts and avoid the risk of each organization developing multiple security architectures that are incompatible with one another. These recommendations complement the "DoD Digital Modernization Strategy," in which DoD CIO has set out a roadmap to support implementation of the National Defense Strategy lines of effort through the lens of cloud, artificial intelligence, command, control, and communications, and cybersecurity. In particular, these recommendations may be used in support of the Digital Modernization Strategy's third goal to "Evolve

[1] "What is a Zero Trust Architecture?" Palo Alto Networks, accessed 10 September 2019, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

Cybersecurity for an Agile and Resilient Defense Posture."[2] Additionally, these recommendations align with DoD's 2018 Cyber Strategy focus on private sector partnerships and network resiliency.[3]

The DIB has previously described[4] zero trust architecture (ZTA) in a white paper titled "The Road to Zero Trust (Security)." That paper was intended for consumption by technical and non-technical network security stakeholders in and out of DoD to provide a common understanding of ZTA principles and terminology, and the following recommendations are intended for policy makers to work in coordination with technical leads within DoD.

The DIB's white paper listed three areas of focus for ZTA, applied at the level of applications and services within the network:

1. User Authentication
2. Device Authentication
3. "Least Privilege Access" Authorization

For user authentication, personnel in DoD currently gain NIPRnet access at the perimeter through hardware-backed MFA using the Common Access Card (CAC). The CAC is recognized throughout DoD networks by drawing from a common database (the Defense Enrollment Eligibility Reporting System, or DEERS). This database includes basic associated attributes, such as personnel category (e.g., contactor, active duty, civilian, etc.), and organization at a high level (e.g., OUSD R&E, OUSD A&S, Army squadron, etc.). SIPRNet similarly relies on hardware-backed MFA using SIPR tokens; like the CAC, a SIPR token grants access at the perimeter of SIPRNet using basic attributes like user name and organization at a high level. Both NIPRNet and SIPRNet rely on domain controllers to field authentication requests, but few of those domain controllers are federated into a common system that can provide authentication for a domain forest. A zero trust user authentication system could leverage any number of identification mechanisms, whether CAC, SIPR token, or other. Regardless of the mechanism, the attributes should ultimately be shared across DoD networks to create a common picture of a user's identity and associated attributes at a more granular level.

For device authentication, DoD must ensure that it conducts consistent scanning and monitoring of devices plugged into NIPRNet across the DoD network ecosystem using standardized health compliance requirements. Without these measures, it would be difficult to run health checks across the network, which presents opportunities for malicious actors to access the network and network resources. This creates a barrier to zero trust implementation, which requires a mapping of the devices seeking access to run health checks on those devices. SIPRNet currently has somewhat better network device awareness than NIPRNet due to the smaller number of devices connected to the network, but both SIPRNet and

---

[2] *DoD Digital Modernization Strategy*, DoD CIO, 12 July 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

[3] "2018 Department of Defense Cyber Strategy," DoD CIO, 18 September 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[4] Kurt DelBene, Milo Medin, and Richard Murray, "The Road to Zero Trust (Security)," Defense Innovation Board, 9 July 2019, https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

NIPRNet should continue to strive for consistent device management standards across the DoD network ecosystem.

DoD authorization currently runs at the local network level, without synchronization to a federated authorization source. At the same time, data and resources are not labeled at a level of granularity that would allow more precise authorization, and as a result, some networks and network enclave access inherently includes promiscuous permissions. This challenge is not unique to DoD: some large companies have a similar structure of locally-managed authorization, but have managed to synchronize the information housed in each local network by applying commercial software solutions that "translate" each local network attribute input into a commonly recognized language. Similarly, commercial companies with a large number of network resources (such as Google) implement more granular data labeling to enable more precise authorization.

These three focus areas should each seek to increase the granularity of attributes assigned to users, devices, data, and applications over time. This detail will allow for more targeted and intentional data transfer, management, and use within network resources, creating contextual checks to ensure that users, devices, data, and applications are appropriately mapped to one another.

Each step carries unique challenges for implementation. The following recommendations provide guidance for zero trust leadership and applying zero trust principles across DoD, using a targeted but scalable method.

1. ZERO TRUST: SYNCHRONIZING EFFORTS

Recommendation 1.1: OSD should prioritize zero trust security architecture and support DoD implementation of zero trust.

- The current state of DoD security architecture is unsustainable. Ongoing security exercises have demonstrated clear vulnerabilities, and these vulnerabilities will only continue to grow as the network attack surface expands. However, DoD runs the risk of getting caught in its own inertia if it fails to respond in a timely manner.

- OSD can prompt rapid action throughout the Department by clearly and consistently listing zero trust implementation as a top priority, while simultaneously assigning clear responsibility for implementation and management.

Recommendation 1.2: OSD should assign specific responsibility within the Department for zero trust network management ("Zero Trust Manager").

- Without a single entity coordinating between the various ongoing zero trust efforts, DoD will likely continue to operate in pockets that loosely adhere to zero trust principles but that are unsynchronized and unable to leverage common access rules.

- The Zero Trust Manager should also formulate and articulate a DoD Network Security Strategy, to include zero trust principles. Based on that strategy, DoD can then identify and acquire commercial products that fit the strategy, rather than cobbling together commercial products without a broader architecture in mind. This will enable DoD to minimize cost and improve the

effectiveness of network security by creating a framework for security product acquisition and implementation.

- To support the Network Security Strategy, DoD should develop a scorecard with metrics to compare relative network security across the Department. These metrics can include items such as: percentage of network devices running anti-virus software, percentage of resources using MFA, number of persistent admin accounts and service accounts, etc.

Recommendation 1.3: Start with critical network resources, building zero trust principles into those points of access before expanding to other network resources.

- It is not necessary to take an "all or nothing" approach to zero trust implementation. This phased approach may encourage more organizations to begin implementing zero trust, but these organizations ultimately need the support and coordination of a Zero Trust Manager to help them prioritize zero trust and implement it quickly and in line with other DoD zero trust efforts.

- Critical resources can be cordoned off using proxies to filter user and device access, gradually moving legacy systems into zero trust compliance.

Recommendation 1.4: Encrypt 100% of data transmitted between devices ("in transit") or stored on mass storage ("at rest"), and promote interoperable encryption across DoD leveraging existing standards (e.g., CNSSP 15[5]).

- Data encryption will require an organization-wide robust and secure encryption key management strategy.

- Encryption is a critical component of zero trust security, as it assumes that the network inherently cannot be trusted and that any data on the network must be guarded accordingly. Going forward, DoD should also consider the risks associated with data in process and encourage encryption for that stage of data management, in addition to data in transit or at rest.

2. USER AUTHENTICATION

Recommendation 2.1: Explore and test the use of more granular user attributes (e.g., work portfolio and projects) using CAC- and SIPR token-based approaches.

- Local networks can develop granular attributes, but these ultimately must be synchronized and updated to a DoD-wide management system.

- The Zero Trust Manager must consistently enforce attribute updating and synchronizing standards for each participating organization to ensure that attribute management systems maintains the most current set of attributes for each user across various networks.

[5] "CNSSP 15: Use of Public Standards for Secure Information Sharing", Committee for National Security Standards, 20 October 2016, https://www.cnss.gov/CNSS/openDoc.cfm?94HhguYr0qU8h1poGDFyag==.

- Access for more granular attributes can be time-limited, depending on the user's required length of the engagement with that resource or data, and system administrators should be able to quickly cut off access if needed at any point during that allotted time…

- ...but time-limitations are only effective if organizational processes for granting access are timely. If users have access blocked and the time to reapply and regain access is prohibitive, users will not be incentivized to build in the granular attributes that would provide more access fidelity.

- User authentication should be "idiot-proofed" to allow for inevitable human error (e.g., do not require long and complex passwords that humans will inevitably write down and leave in plain sight). In the long term, DoD should consider solutions like biometric authentication to mitigate this risk.

Recommendation 2.2: Lift the burden of authentication off individual local networks and network resources by giving responsibility to federated identity provider/manager.

- Active Directories (AD) across DoD are currently not federated into a forest, which would help synchronize authentication across networks. This function could be managed by a third party identity management provider (commercial sector has multiple options for such a manager).

- AD federation has sometimes been met with hesitancy (both in DoD and the commercial sector) due to lack of trust between network enclaves. Federation is viewed by some as a vulnerability because network access frequently comes with automatic access to certain network resources, which makes each organization reluctant to link up with new users and devices that do not require direct access to their networks. AD federation may be more palatable once individual enclaves take more proactive steps to build in granular identity attributes and enforce device compliance. Network access should not be associated with any automatic resource access inside the network, which will reduce the perceived risk of federation.

Recommendation 2.3: Replace standing administrative authorities with temporal, task-dependent administrative authorities.

- No user should be granted "super user" privileges with broad-brush, constant access. Users should receive selective access as necessary, which can then be removed when the user has completed his or her administrative task.

Recommendation 2.4: Invest in R&D and pathfinder for "classification as an attribute," where user clearance level can be used as a check to grant access to specific data within network resources.

- DoD should explore the possibility of converging NIPRNet and SIPRNet onto the same network, relying on zero trust principles to guard access and building in user clearance level as a core attribute for access. Both NIPRNet and SIPRNet should adopt the perimeter security measures of SIPRNet to maintain the higher level of perimeter security as an initial barrier to entry.

Recommendation 2.5: Develop a common strategy across DoD organizations for integrating non-DoD users (e.g., defense contractors, allies, and partners without CACs) into the network ecosystem, relying on zero trust principles as a baseline for users and devices.

- DoD is already investigating and pursuing options to better integrate non-DoD users into DoD networks while maintaining zero trust security standards (e.g., DoD Enterprise DevSecOps Initiative). DoD should continue to seek out CAC alternatives that are consistently applied across the defense industrial base, relying on zero trust best practices (e.g., MFA, time-limited access with the option to quickly remove access as needed).

- DoD should also continue to investigate methods of better integrating allies and partners without U.S. citizenship into operations by providing narrow, targeted network access as needed.

3. DEVICE AUTHENTICATION

Recommendation 3.1: Consistently scan NIPRNet and SIPRNet for all devices connected to each network.

- Zero trust architecture for DoD requires a comprehensive device inventory tracking all devices connected to NIPRNet and SIPRNet, similar to how the DEERS database tracks all DoD users.

- The device scanning/management process can (and should) be phased across networks, rather than trying to implement across the whole of DoD in one pass. Organizations should identify high value assets on their networks and focus on scanning/managing devices that connect to those assets.

- Scan and monitor devices connected to networks to identify unhealthy/non-compliant devices, then either cut off their access or remove devices altogether.

Recommendation 3.2: Ensure consistent and robust device-use logging across networks and network enclaves to detect patterns of user behavior on specific devices, and flag anomalies in behavior for administrators to monitor

- Logging and monitoring of network traffic and user/device behavior on the network should be standardized across DoD. This will provide a better understanding of network mapping and make it easier to identify anomalous behavior that may indicate unsanctioned access to network resources.

Recommendation 3.3: Use SIPRNet as a foundation to build "portability-centric" device management (focused on mobile phones, laptops, etc.). Portable network devices should be required to meet health and configuration compliance requirements, and these standards should ultimately be applied to non-portable devices as well.

- SIPRNet currently has a limited number of portable devices associated with its network. This provides a "blank slate" to enforce compliance for any new portable devices added to the network, while also encouraging the network as a whole to reduce reliance on closed physical locations as a source of security. As part of this effort, all portable devices should be required to encrypt data at rest as well as in transit.

- DoD should ultimately apply this "portability" model more broadly, so that all devices (e.g., desktops) have the same compliance requirements, whether portable or not.

Recommendation 3.4: Ensure that DoD runs regular and consistent device health checks throughout its networks, leveraging existing commercial solutions to monitor device compliance and drive device reconfiguration if not in compliance.

- Various commercial solutions exist that can solve for this challenge, e.g., antivirus software. DoD should be able to apply commercial solutions with minimal alteration.
- Commercial solutions will help identify unhealthy/non-compliant devices. These devices should either have access cut off until they come into compliance or be removed altogether. This "Comply to Connect" (C2C) approach has been explored throughout DoD, but needs to be enforced to provide a baseline of network security.
- In addition to checking device health upon request for access, network should run regular device health reviews to maintain a baseline of security. The faster the rate of reviews, the better.

4. "LEAST PRIVILEGE ACCESS" AUTHORIZATION

Recommendation 4.1: Deploy existing commercial solutions to "translate" local network attribute inputs into a single federated authorization source.

Recommendation 4.2: Label data and resources throughout DoD networks at a more granular level to enable more precise authorization for users and devices requesting access, limiting promiscuous permissions.

- The Defense Digital Service (DDS) is currently working to design zero trust "wrappers" that can be placed around network resources to run authentication and authorization in a more targeted way. The Zero Trust Manager should coordinate with DDS to validate this concept and consider implementation steps for broad deployment across DoD.

Recommendation 4.3: Decouple user and device location from authorization. The connection point should not drive access (e.g., connecting at the Pentagon should not provide any automatic access beyond basic internet connection).

- Instead, access should largely depend on the identity attributes of the user and device, in addition to basic checks on device configuration compliance and encryption standards.