Carnegie Mellon University
Software Engineering Institute

WHAT ARE THE DIFFERENCES BETWEEN DEPARTMENT OF DEFENSE (DOD) ZERO TRUST REFERENCE ARCHITECTURE VERSION 1.0 AND 2.0?

Timothy Morrow

July 2023

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Introduction

The Department of Defense (DoD) produced version 1.0 of the Zero Trust Reference Architecture (ZTRA) in February 2021 which directed next generation cybersecurity architectures to become data centric and based upon zero trust (ZT) principles. Version 2.0 of the ZTRA was released in July 2022. This paper provides a little background on the original document, then identifies the changes that were made in the new version.

Version 1.0 February 2021 Highlights

ZTRA identified five major tenets of ZT:

1. Assume a hostile environment.
2. Presume breach.
3. Never trust, always verify.
4. Scrutinize explicitly.
5. Apply unified analytics.

ZTRA has seven ZT pillars:

1. user
2. device
3. network or environment
4. application & workload

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

5. data
6. visibility & analytics (considered cross-cutting capability in CISA ZT Maturity Model (ZTMM))
7. automation & orchestration (considered cross-cutting capability in CISA ZTMM)

A governance cross-cutting capability is overarching across the seven pillars.

The ZTRA maturity model identified three protection levels (baseline, intermediate, advanced); each with a set of descriptions that define the protection level. The maturity model defined two processes (discovery and assessment) for organizations to use to prepare for transitioning to ZT strategy.

ZTRA used the DoD Architecture Framework (DoDAF) to visualize and discuss applying a ZT strategy for DOD enterprise architectures. The following DoDAF viewpoints were used:

1. OV-1 High Level Operational Concept Graphic
2. CV-1 Vision
3. CV-2 Capability Taxonomy
4. StdV-1 Standards Profile
5. StdV-2 Standards Forecast
6. CV-4 Capability Dependencies
7. CV-6 Capability to Operational Activities Mapping
8. CV-7 Capability to Services Mapping
9. OV-2 Operational Resource Flow Description
10. OV-5b Operational Activity Model
    a. Eight of these viewpoints were used to describe ZT operational activities, workflows, requirements, task analysis, operational planning, and analysis of information workflows.
11. AV-2 Integrated Dictionary

These viewpoints provided a starting point for applying ZT for DoD enterprise networks. The viewpoints identified capabilities, functions, activities, and information exchange which networks designers and maintainers need to consider when moving to ZT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

ZTRA expanded upon the existing DoDAF viewpoints by providing additional operational and services views, as well as adding OV-6a Operational Rules Model viewpoints were added which identified seven guiding principles for the reference architecture. These views provide context to what needs to be considered when applying ZT. ZTRA provided architecture patterns in the form of DoDAF SV-1, SvcV-1, and SvcV-2 viewpoints, as well as transition architecture planning guidance, which starts with as-is and moves through a transition to a target architecture.

1. Assume no implicit or explicit trusted zones in networks.
2. Identity-based authentication and authorization are strictly enforced for all connections and access to infrastructure, data, and services.
3. Machine-to-machine (M2M) authentication and authorization are strictly enforced for communication between servers and the applications.
4. Risk profiles that are generated in near-real-time from monitoring and assessing both user and devices behaviors are used in authorizing users and devices to resources.
5. All sensitive data is encrypted both in transit and at rest.
6. All events are to be continuously monitored, collected, stored, and analyzed to assess compliance with security policies.
7. Policy management and distribution is centralized.

ZTRA identified 11 use cases, which provides more specific guidance concerning ZT strategies.

1. data-centric security protections
2. data encryption protections
3. coordinating policy for data-centric security protections
4. data analytics & AI
5. centralized orchestration & policy management
6. dynamic, adaptive policy feedback loop
7. VPN-less implementation
8. east-west segmentation
9. global uniform device hygiene
10. dynamic, continuous authentication
11. conditional authorization

This additional information provides the next level down information to what is needed to define what ZT means to DoD network over the previous version. ZTRA discussed the application and assessment

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

of data and security governance policies to support ZT implementation in systems. This starts the discussion concerning mature ZT implementations.

Legal Markings

Copyright 2023 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

DM23-0661

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.