Carnegie Mellon University
Software Engineering Institute

ZERO TRUST INDUSTRY DAY 2022: AREAS OF FUTURE RESEARCH

Matthew Nicolai, Trista Polaski, and Tim Morrow
January 2023

In August 2022, the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) hosted *Zero Trust Industry Day 2022* to enable industry stakeholders to share information about implementing zero trust (ZT). At the event, attendees focused on how federal agencies with limited resources can implement a zero trust architecture (ZTA) that adheres to executive orders M-22-009 [White House 2022] and M-21-31 [White House 2021], both of which address federal cybersecurity measures.[1]

As discussed in a previous SEI white paper, ZTA "has emerged as an important topic of discussion in both the public and private sectors" [Nicolai 2022]. To manage internal and external threats, the ZT security strategy applies the principles of micro-segmentation and least privilege. Through authentication and authorization, ZT regulates interactions among users, devices, networks, and data.

The ZT approach marks a major shift from the traditional perimeter-based security model commonly used today. Many federal agencies are shifting toward ZTA, and more government and private sector organizations are following suit. ZT vendors are focusing heavily on ZTA, a relatively new area of cybersecurity, in an effort to help organizations shift to ZT.

At the SEI, our goal for the 2022 event and future ZT industry days is to encourage information sharing and discussion among organizations that are developing hardware or software ZTA solutions. The 2022 event featured keynote addresses; presentations from ZT vendors; a Q&A session; and panel discussions among experts from government, industry, and research leaders. During these discussions, participants identified ZT-related issues that could benefit from additional research. By focusing on these areas, organizations in government, academia, and industry can collaborate to develop solutions that streamline and accelerate ongoing ZTA transformation efforts. In this paper, we discuss some of these potential research areas.

[1] OMB M-22-09 calls for "a Federal Zero Trust Architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of FY 2024 to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns" [Whitehouse 2022].

Area 1: Agree on a Generally Accepted Set of Basic ZT Definitions

According to SP 800-207, *Zero Trust Architecture,* ZT access decisions are made on a *per-session* basis [NIST 2020]. However, there are several definitions of the term *session*, and panelists at the Zero Trust Industry Day 2022 event emphasized the importance of defining that and other terms, including *per session*, *per-request access*, and *per-request logging*.

Paul Martini of iboss, a panelist at the SEI event, described a *session* as a central concept in ZTA that generally refers to the specific instance when a user gains access to an enterprise resource [Martini 2022].

Although NIST SP 800-207 states that access decisions are made on a per-session basis, NIST also released CSWP 20, which explicitly states that "the unit of 'session' can be nebulous and differ depending on tools, architecture, etc." [Rose 2022]. NIST further describes a *session* as a "connection to one resource utilizing one network identity and one privilege for that identity (e.g., read, write, delete, etc.) or even a single operation (similar to an API call)." However, since this definition may not always correspond to real-world implementations, NIST also defines *session* more generally: "[a] connection to a resource by a network identity with set privileges for a set period of time" [Rose 2022].

This broader definition states that reauthentication and reauthorization are periodically required in response to privilege escalation, timeouts, or other operational changes to the status quo. Similarly, comprehensive definitions are also needed for other concepts (e.g., *per-request access* and *per-request logging*). Defining, standardizing, and reinforcing these concepts will help to solidify the industry's overall understanding of ZT tenets and how they will look in practice.

Area 2: Establish a Common View of ZT

From an operational perspective, organizations can benefit from an established, open source standard for defining event communication between ZT components. Organizations must also understand how they can leverage new and existing frameworks and standards to maximize ZT interoperability and efficacy.

Using a common protocol could allow greater integration and communication among individual components of a ZT environment. At the SEI event in August, Jason Garbis from Appgate suggested a notable example of such a protocol: the OpenID Foundation's Shared Signals and Events (SSE) Framework. That framework helps standardize and streamline the communication of user-related security events among different organizations and solutions.

Another area worth exploring is policy decision points (PDPs) and related elements used throughout an enterprise environment. Existing solutions may leverage unique workflows to develop instruction sets or operating parameters for the PDP. For access-related decisions, the PDP relies on policies, logs, intelligence, and machine learning (ML); however, there is little discussion about how these factors might work in practice and how they should be implemented. To encourage uniformity and

interoperability, security organizations could develop a standardized language for PDP functionality, similar to the STIX/TAXII[2] standards developed for cyber threat intelligence.

Area 3: Establish Standard ZT Maturity Levels

Existing ZT maturity models do not provide granular control or discussion of the minimal baselines required for effective shifts to ZT. It is important to consider how to develop a maturity model with enough levels to help organizations identify exactly what they must do to meet ZT standards for basic security.

At the SEI event in August, Jose Padin from Zscaler emphasized the need to define the minimum baseline requirements necessary for ZTA in the real world. It is critical to establish a standard of technical requirements for ZT maturity so that organizations can identify and audit their progress toward digital trust.

In his presentation, Jose highlighted some of the strengths of the *CISA Zero Trust Maturity Model*, which features several pillars depicting the various levels of maturity in the context of ZT [CISA 2021].[3]

The CISA model helps organizations visualize best practices and their associated maturity levels, but there is still considerable uncertainty about what the minimum requirements are to achieve ZT. Organizations cannot assess their current state of ZT maturity and choose their best course of action without clear criteria to compare against.

The CISA ZT maturity model progresses from Traditional to Advanced to Optimal, which may not provide enough granular insight into the middle ground where many organizations will likely find themselves during the transitional phases of ZT transformation. Furthermore, while CISA's model defines the policies and technologies that determine each level of maturity, there is minimal technical discussion about how these concepts might look and work in practice.

It is necessary to (1) address the stratification of ZT maturity and (2) provide organizations with sufficient reference materials and guidance so they understand where they currently stand (i.e., their "as-is" state) and where they need to go (i.e., their "to be" state). Organizations would benefit from more information about how to implement ZT strategies across their digital assets to achieve compliance, similar to the concept of a minimum viable product.

---

[2] Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information

[3] For a high-level view of CISA's Zero Trust Maturity Model, refer to Figure 2 (page 5) of *Zero Trust Maturity Model* [CISA 2021].

Area 4: Explain How to Progress Through ZT Maturity Levels

For successful ZT transformation, it is critical to do the following:

- Understand the specific steps an organization must take.
- State the transformation process directly and logically.
- Identify how organizations can achieve digital trust.

Building on *Area 3: Establish Standard ZT Maturity Levels*, organizations in the security space must identify the minimum steps required to implement ZT at some level while also demonstrating how those steps might look in practice. Once an organization has begun implementing ZT, it can work toward higher levels of ZT maturity, with the ultimate goal of achieving digital trust.

According to the Information Systems Audit and Control Association (ISACA), *digital trust* refers to the "confidence in the integrity of the relationships, interactions and transactions among suppliers/providers and customers/consumers within an associated digital ecosystem" [ISACA 2022]. In essence, ZT serves as the foundation for interaction among entities from a cybersecurity perspective. Digital trust encompasses all the interactions between internal and external entities more comprehensively.

Implementing ZT and achieving digital trust require strong collaboration between government and private sector organizations. Government and related entities must actively collaborate with private sector organizations to align models, standards, and frameworks with real-world products and services. This approach provides end users with useful information about how a particular product can leverage ZT strategies to achieve digital trust. These collaborations must focus on (1) identifying what a particular security offering can and cannot do and (2) how each offering can integrate with others to achieve a specific level of compliance. This information enables organizations to act more quickly, efficiently, and effectively.

Area 5: Ensure ZT Supports Distributed Architectures

With the increasing adoption of cloud solutions and distributed technologies (e.g., content delivery networks [CDNs]), it is necessary to develop security frameworks that account for applications and data moving away from a central location and closer to the user.

When developing frameworks and standards for the future of ZT, it is important to consider that offsite data storage is being moved closer to the consumer, as demonstrated by the prevalence of CDNs in modern information technology (IT) infrastructures.

At the SEI's August event, Michael Ichiriu of Zentera suggested that researchers consider exploring this topic in the context of new security frameworks since many existing frameworks take a centralized data center/repository approach when describing security best practices [Ichiriu 2022]. This approach underserves CDN-oriented organizations when they are developing and assessing their security posture and architecture.

Area 6: Establish ZT Thresholds to Block Threats

In a ZT environment, it is important to understand what constitutes the minimum amount of information required to effectively isolate and block an activity or piece of malware. Identifying this information is critical since a growing number of ransomware attacks are using custom malware. To defend against this threat, organizations must improve their ability to detect and block new and adapting threats. An important aspect of ZT is using multiple strategies to detect and isolate attacks or malware before they spread or cause damage.

As its name suggests, ZT should not trust unknown software, updates, or applications, and it must quickly and effectively validate unknown software, updates, and applications. ZT can use a variety of methods (e.g., sandboxes and quarantines) to test and isolate new applications. These results must then be fed into the PDP so that future requests for those applications can be approved or denied immediately.

Area 7: Integrate ZT and DevSecOps

In the development process, it is important to use as many security touchpoints as possible, especially those related to ZT. It is also important to understand how to emphasize the importance of security in an organization's development pipeline for both conventional and emerging technologies.

These considerations lead us into the realm of DevSecOps, which refers to a "set of principles and practices that provide faster delivery of secure software capabilities by improving the collaboration and communication between software development teams, IT operations, and security staff within an organization, as well as with acquirers, suppliers, and other stakeholders in the life of a software system" [SEI 2023].

As automation becomes more prevalent, DevSecOps must account for the possibility that a requestor is automated. ZTA uses the identity of the workloads that are attempting to communicate with one another to enforce security policies. These identities are continuously verified; unverified workloads are blocked and therefore cannot interact with malicious remote command-and-control servers or internal hosts, users, applications, and data.

Historically, when developing software, everyone assumed that a human would be using it, and when security was implemented, default authentication methods were designed with humans in mind. However, as more devices connect with one other autonomously, software must be able to use ZT to integrate digital trust into its architecture. To enable the ZT strategy, DevSecOps must be able to answer the following questions:

- Is the automated request coming from a trusted device?
- Who initiated the action that caused the automated process to request the data?
- Did an automated process kick off a secondary automated process that is now requesting the data?
- Does the human who configured the automated processes still have access to their credentials?

Area 8: Set Business Expectations for ZT Adoption

Security initiatives are frequently expensive, which contributes to the organization's perception of security as a cost center. It is important to identify inefficiencies (e.g., obsolescence) during the ZT transformation process. It is also critical that organizations understand how to use ZT to maximize their return on investment.

ZT is a strategy that evaluates and manages the risk to an organization's digital assets. A ZT approach shifts the defenses from the network perimeter to in-between digital assets and requires session authentication for all access requests. Many ZT strategies can be implemented with a reasonable amount of effort and at a low cost to the organization. Examples include micro-segmentation of the network, encryption of data at rest, and user authentication using multi-factor authentication.

However, some solutions (e.g., cloud environments) require a lengthy transition period and incur ongoing costs. Since organizations have unique risk tolerance levels, each organization must develop its own ZT transformation strategy and specify the initial phases. Each of these strategies and phases will have different costs and benefits.

Summary

The SEI's Zero Trust Industry Day 2022 was designed to bring vendors in the ZT field together and offer a shared platform for discussion. This approach allowed participants to objectively demonstrate how their products could help organizations with ZT transformation. Discussions included several areas that could use more exploration. By describing these areas in this paper, we at the SEI are raising awareness, promoting collaboration among public and private sector organizations to solve real-world problems, and accelerating ZT adoption in both government and industry.

References

[CISA 2021]

Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model. *Cybersecurity and Infrastructure Security Agency (CISA) website*. January 2023 [accessed]. https://www.cisa.gov/zero-trust-maturity-model

[Ichiriu 2022]

Ichiriu, Mike. Zentera Materials for the 2022 Zero Trust Industry Day. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887552

[ISACA 2022]
Information Systems Audit and Control Association. *New ISACA Guide Outlines Key Components of Digital Trust Implementation*. May 2022. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2022/new-isaca-guide-outlines-key-components-of-digital-trust-implementation

[Martini 2022]
Martini, Paul. iboss Materials for the 2022 Zero Trust Industry Day. August 2022. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887542

[Nicolai 2022]
Nicolai, Matthew; Richmond, Nate; & Morrow, Tim. Industry Best Practices for Zero Trust Architecture. Software Engineering Institute. December 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=890254

[NIST 2020]
National Institute of Standards and Technology (NIST). *Zero Trust Architecture.* NIST SP 800-207. August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[Rose 2022]
Rose, Scott. *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators*. May 2022. https://doi.org/10.6028/NIST.CSWP.20

[SEI 2023]
DevSecOps. *Software Engineering Institute Website*. January 2023 [accessed]. https://www.sei.cmu.edu/our-work/devsecops/

[White House 2021]
The White House. *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*. OMB M-21-31. Office of Management and Budget (OMB). 2021. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[White House 2022]
The White House. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. OMB M-22-09. Office of Management and Budget (OMB). 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Legal Markings

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.

DM23-0061

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