Using a Scenario to Reason About Implementing a Zero Trust Strategy

Tim Morrow
Rhonda Brown
Elias Miller

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Using a Scenario to Reason About Implementing a Zero Trust Strategy

© 2024 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.

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.

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 use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM24-0515
Overview

Security model developed by John Kindervag and team at Forrester approximately 2009.

Goals

• Remove implicit trust.
• Move security from the network to users, applications, and workloads.

NIST Special Publication 800-207 Zero Trust Architecture
• Identifies Zero Trust Architecture (ZTA) as a strategy

Zero Trust will be a journey.

[NIST 800-207 2020]
Principles

Ensure all resources are accessed securely, regardless of location.
Adopt a least privilege strategy and strictly enforce access control.
Inspect and log all traffic.
Ensure all components support application programming interface (API)s for event and data exchange.
Automate actions across environments and systems, driven by context and events.
Audit continuously.
Working Definition

A zero trust system is an *integrated security platform* that uses *contextual information* from identity, security and IT infrastructure, and risk analytics tools to inform and enable the *dynamic enforcement of security policies uniformly across the enterprise*.

Zero trust shifts security from an ineffective perimeter-centric model to a *resource- and identity-centric model*. As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility.

[Zero Trust Security 2021]
NIST Zero Trust Architecture Components
Policy Enforcement Point Types
Resource-Based Deployment Model

[Zero Trust Security 2021]
Enclave-Based Deployment Model

Control Plane

Device
PEP

Subject

Data Plane

Resource Enclave
Implicit Trust Zone

[Zero Trust Security 2021]
Cloud-Routed Deployment Model
Zero Trust Planning

Strategy Comes First, Understanding Your Data Comes Next.

- Defining the authorizations, conditions, and entitlements to access data represents approximately 83% of ZT implementation costs. (Based on Greg Touhill’s research at CMU’s Heinz College)

Adopt the Zero Trust security strategy

- “Zero Trust is the starting point on the road to Digital Trust”
- People, Process, Technology (aka hw/sw/wetware)
- The strategy applies everywhere: Enterprise Information Technology (EIT), Operational Technology (OT), Industrial Control System (ICS), Internet of Things (IoT), & Spectrum (i.e., 5G/6G)

[Understanding Zero Trust 2022]
Software Engineering Institute (SEI) Zero Trust Journey

SEI Cybersecurity Engineering Assessments

Prepare
- Strategy
- Infrastructure
- Budget
- Roadmap
- Executive Endorsement

Plan
- Asset Inventory
- Subject Inventory
- Data Inventory
- Data Flow Inventory
- Workflow Inventory
- System Security Engineering
- Monitoring Changes

Assess
- Maturity
- Gaps
- Risk
- Subject Inventory Pilot
- Data Flow Inventory Pilot
- Workflow Inventory Pilot

Implement
- Policy Development
- Communicate and Coordinate
- Deploy
- Operate
- Monitor and Measure
- Change Management
Common Challenges

Governance
• Inventories (asset, subject, data, data flow, workflow, APIs)

Architecture
• Awareness and accuracy

Cost
• Adoption cost

Measurement
• What is success?
Zero Trust Guidance Documents
## CISA Zero Trust Maturity Model

<table>
<thead>
<tr>
<th>(maturity stages)</th>
<th>Identity Pillar</th>
<th>Devices Pillar</th>
<th>Networks Pillar</th>
<th>Applications and Workloads Pillar</th>
<th>Data Pillar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility and Analytics</td>
<td></td>
<td>Automation and Orchestration (cross cutting)</td>
<td>Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility and Analytics</td>
<td></td>
<td>Automation and Orchestration (cross cutting)</td>
<td>Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visibility and Analytics</td>
<td></td>
<td>Automation and Orchestration (cross cutting)</td>
<td>Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traditional</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[CISA ZTMM 2023]
Example: CISA Zero Trust Maturity Model Identity Pillar Functions

<table>
<thead>
<tr>
<th>Function</th>
<th>Traditional</th>
<th>Initial</th>
<th>Advanced</th>
<th>Optimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Agency authenticates identity using either passwords or multi-factor authentication (MFA) with static access for entity identity</td>
<td>Agency authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity)</td>
<td>Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password</td>
<td>Agency continuously validated identity with phishing-resistant MFA, not just when access is initially granted.</td>
</tr>
<tr>
<td>Risk Assessments</td>
<td>Agency makes limited determinations for identity risk (i.e., likelihood that an identity is compromised).</td>
<td>Agency determines identity risk using manual methods and static rules to support visibility.</td>
<td>Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.</td>
<td>Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.</td>
</tr>
</tbody>
</table>
DoD Zero Trust Strategy
## DoD Zero Trust Maturity Model

### Discovery
- Identify Data, Assets, Applications, Services (DAAS)
- Map data flows
- Inventory User and Devices
- Identify privilege accounts
- Log network traffic

### Baseline
- Access to DAAS is determined by cybersecurity policy
- Networks are segmented with deny all/permit by exception
- Devices are managed and compliant to IT security policies
- Implement least privileged access
- MFA technologies are in use
- Begin data classification and tagging of critical data
- Meet encryption requirements

### Assessment
- Determine compliance state leveraging existing hardening standards
- Determine proper account privilege levels
- Identify, if existing network/environment security policies as implemented in least privilege manner

### Intermediate
- Enhanced cybersecurity policies are used to determine access based on fine-grained user and device attributes
- Micro-segmentation across majority of network
- User identity based on Enterprise Federated Identity Service
- Enhance LPA with privileged access mgmt.
  solution
- Initial DLP and DRM implementations
- Data is tagged and classified via flow analysis and simple automation
- User and Entity Behavior Analytics (UEBA) to develop baseline

### Advanced
- Cybersecurity policies dynamically determine access to DAAS, driven by robust real-time analytics
- Full micro-segmentation
- Continuous and adaptive authentication and authorization
- User and device identity based on Enterprise Federated Identity Service
- Fully implemented Just-in-Time and Just-Enough access policy
- Majority of data is tagged and classified through machine learning
- Full DLP and DRM implementation incorporating data tags
- Advanced analytics enable automated and orchestrated threat detection

[DISA/NSA 2022]
How to Develop the Context Necessary to Apply ZT?

Mission Engineering (ME) is the planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects.

Five Objectives

1. Enable mission-focused, threat-informed analysis.
2. Identify and address mission gaps.
3. Develop Government Reference Architectures (GRA) to guide development and prototypes.
4. Inform stakeholders how the architecture is envisioned to address/support the missions.
5. Generate and capture scenarios, assumptions, constraints, system attributes, and data for use during analysis.
Using a Scenario to Reason About Implementing a Zero Trust Strategy

Define Security Objectives
Define Life Cycle Security Concepts
Define Success Measures

Define Security Requirement
Define Security Aspects of the Solution
Realize the Security Aspects of the Solution
Produce Evidence for Security Aspects of the Solution

Produce Evidence for Security Aspects of the Problem

Develop Assurance Case for Acceptable Security
Demonstrate Assurance Case is Satisfied

Figure 10

System Security Analyses
Concepts, Principles, Means, Methods, Processes, Practices, Tools, Techniques
Zero Trust Industry Day Event

- Organizations who develop solutions for implementing a zero trust architecture get together and share their ideas, solutions, and experiences
- The SEI asked developers of zero trust solutions how they would solve a problem in a situation that requires cyber protection of data and resources.
- Presenters from each participating organization prepare a 1-hour presentation and address challenges in complying with requirements from six guidance documents.
  - CISA Zero Trust Maturity Model, Version 2.0
  - DoD Zero Trust Strategy
  - National Cybersecurity Strategy
  - OMB M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents
  - OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
  - CISA Zero Trust Implementation Strategy
Zero Trust Industry Day 2022 Scenario

A fictional company operating a hybrid, multi-cloud enterprise.
• two legacy systems
• one database containing Protected Personal Information (PPI)
• four different identity and access management systems
• lacks a centralized security operations center (SOC)
• budget of $3 million and a one-year timeline during which it must start to address Office of Management and Budget (OMB) memoranda

SEI was looking for approaches to zero trust that also address challenges in complying with OMB memoranda.
• OMB M-21-31, Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents
• OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
Panel discussions:
- What areas of zero trust need further research?
- What areas do not need further research?
- What are you tired of hearing about from your customers about zero trust?
- Given the SEI’s role as an honest broker, what do you suggest that the SEI can do to help you in your work in zero trust?

Key Takeaways:
- The Q&A panel session spurred good conversation, where people were free to be honest and talk about their experiences.
- Resulted good networking and teaming among solution providers.
- Hearing the challenges of solution providers.
- Take away for attendees is to not look for a single solution provider to do it all.
  - Many focus their development in one particular zero trust area, e.g., ICAM, segmentation.
  - Need contextual awareness, priorities, before going to solution provider to fill that part of ZT
Zero Trust Industry Day 2024 Scenario

This year’s scenario integrates manufacturing with smart city technologies. Involves a fictitious chip manufacturing facility in a city on an island that integrates smart technologies into its infrastructure.

- Three legacy OT Systems
  - controlling the “clean room”, production of silicon wafers, SCADA system for monitoring
- Facility reliance on OT/IIoT
  - Smart sensors and actuators are connected through the internet to industrial applications
- Smart City reliance on IoT (IoT enabled devices hardware)
  - waste management systems, public transportation systems, traffic management systems
- Heterogenous environments
- Hosted private cloud residing on-premise at facility
- Public Cloud used by manufacturing facility and internet activity in smart city
- Connected Services
  - centralized Identity, credential, and access management (ICAM) service, remote from island
  - cellular and Wi-Fi coverage with 5G capability
  - Satellite network
Scenario Concerns to Address

Handling vulnerabilities and threats in highly connected systems. What concerns do they create?

- Disruption of connectivity
  - ICAM – loss of cloud services, loss of satellite communication
- Ensuring solutions do not impair accessibility and availability for manufacturing environment
- Legacy OT systems
  - security in standard industrial communication protocols
  - older components do not support encryption.
  - devices not designed with security required for internet
  - devices built with a back door for calibration
  - common password for all devices
- IoT and IIoT systems
  - IIoT technology running on older infrastructure
  - vulnerable intercommunication among IIoT devices
  - smart city IoT devices weak on security from the manufacturer
SEI Zero Trust Collection

Our Zero Trust collection contains SEI zero trust publications, including newsletters, blog posts, podcasts, webcasts, presentation videos from our Zero Trust Industry Days events, and related materials of interest.

https://insights.sei.cmu.edu/library/zero-trust-collection/

Information about our Zero Trust Industry Days 2024 event:
Fact Sheet
https://insights.sei.cmu.edu/documents/5851/zero_trust_days.pdf
Scenario
https://insights.sei.cmu.edu/library/zero-trust-industry-day-2024-scenario-secluded-semiconductors-inc/
Web pages
https://resources.sei.cmu.edu/news-events/events/zero-trust/
References
References –1

[CISA ZTMM 2023]

[DISA/NSA 2022]

[NIST 800-207 2020]
https://csrc.nist.gov/publications/detail/sp/800-207/final
References –2

[NMM-2022-01A1]  

[Understanding Zero Trust 2022]  

[Zero Trust Security 2021]  

[MEG]  
Contact Information

Tim Morrow
CERT Division Situational Awareness Technical Manager
tbm@sei.cmu.edu
412.268.4792

Rhonda Brown
CERT Division Situational Awareness Senior Solutions Engineer
rbrown@cert.org
412.268.3963

Elias Miller
CERT Division Situational Awareness Assistant Solutions Engineer
emiller@cert.org
412.268.6453