Zero Trust Architecture

A presentation by:

Lindsey Wingate
Jesse Van Den Berg

USC Viterbi
School of Engineering

Table of Contents

1. Background
2. NIST SP 800-207, Zero Trust Architecture
3. ZTA Implementation
4. Real-world Example of ZTA
5. Tenets of ZTA
6. ZTA as a solution
7. ZTA vs RM vs RVM
8. ZTNA Examples
9. Advantages
10. Disadvantages
11. References

Background

- Stuxnet virus, Supervisory Control and Data Acquisition, 2010
- Cyber attack on Ukraine’s power grid, 2015
- Office of Personnel Management, data breach 2015
- Perimeter -based security measures such as firewalls, intrusion detection systems (IDS), or intrusion prevention systems (IPS) at the network border failed to prevent these attacks.
- Additionally, once attacks were authenticated and trusted in the internal network there were no long-term means to defend against these types of sabotage.
- Zero Trust and Software-Defined Networking Steering Group 2018
- Zero Trust Architecture documentation (ZTA), National Institute of Standards and Technology 2022

NIST SP 800-207

- “No trust, always verify”
  - (i.e. Zero trust)
- Focus based on protecting resources rather than the network
- Assumes attacker is present in the environment

Implementing Zero Trust

1. Restricting resources to those who need them
2. Allowing minimal access only
3. Implementing policy decision points (PDP) and policy enforcement points (PEP) for authentication and authorization
4. “implicit trust zones”

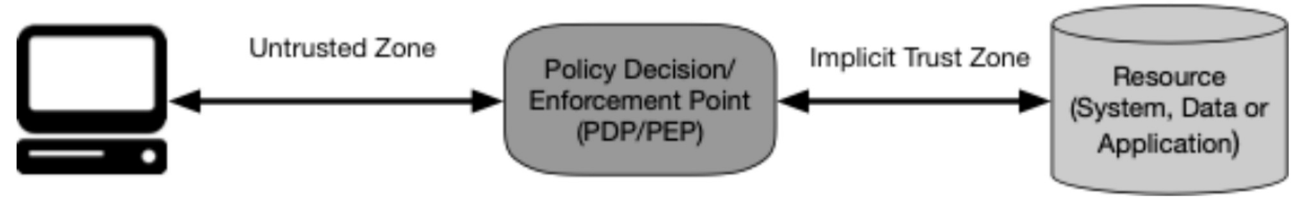
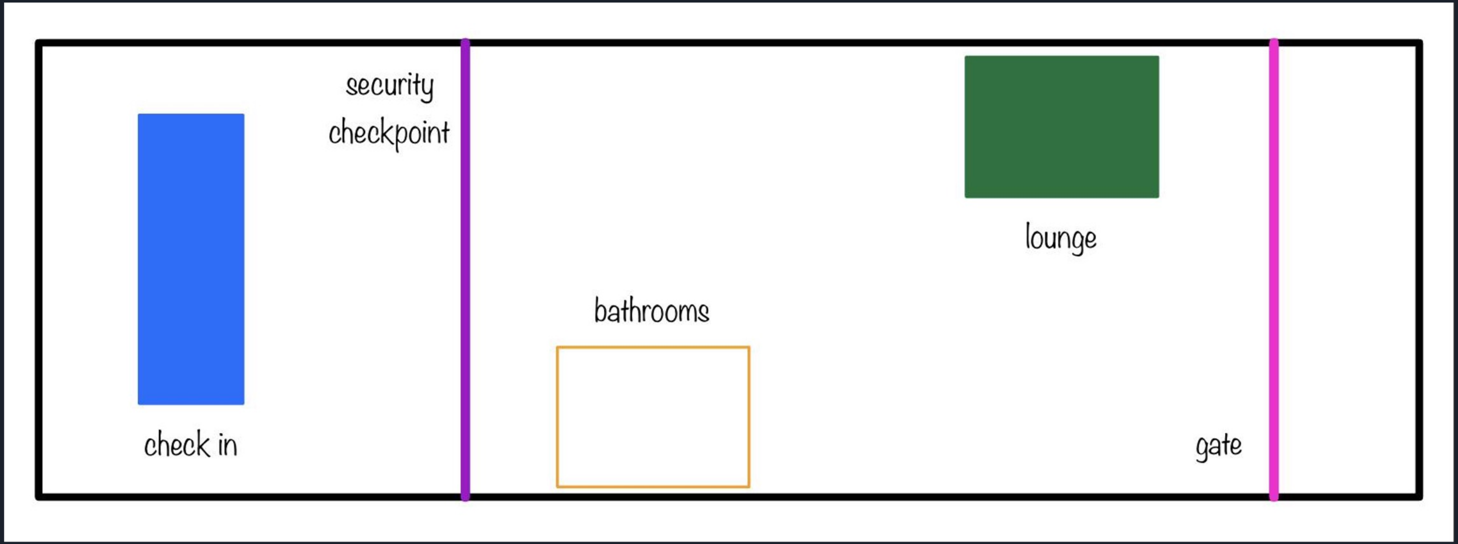

Untrusted Zone
Policy Decision/ Enforcement Point (PDP/PEP)
Implicit Trust Zone
Resource (System, Data or Application)

Figure 1: Zero Trust Access

Airport Model

(ZTA)



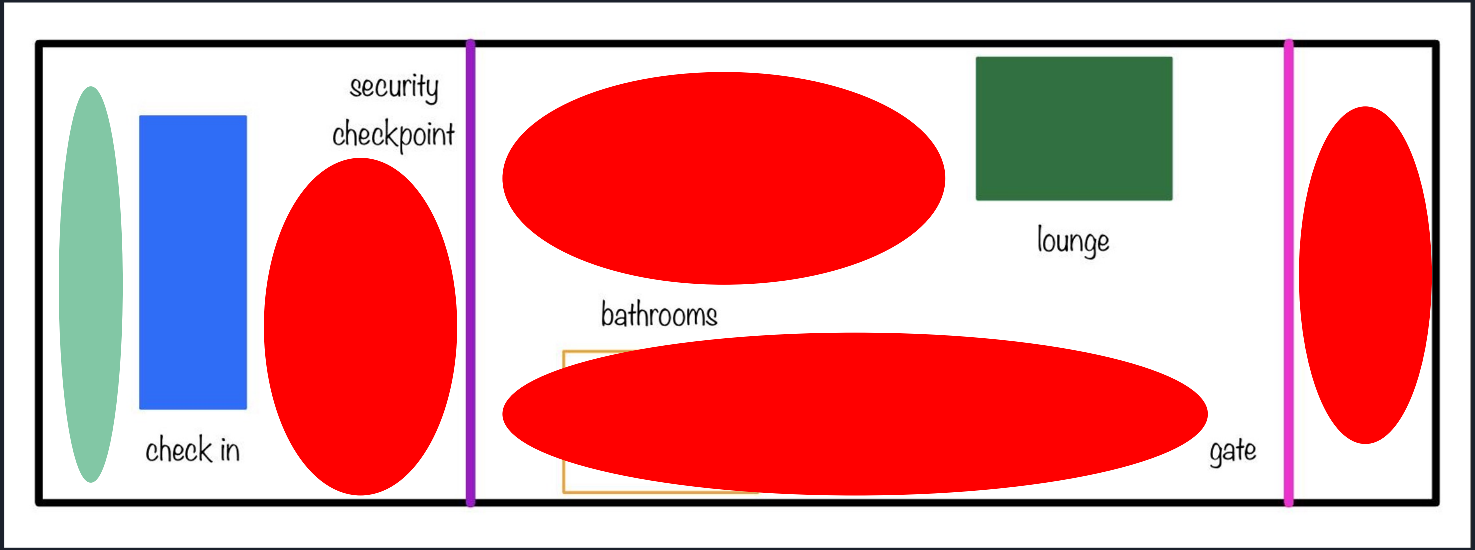
Airport Model
(ZTA)

Allice

Implicit Trust zones

Bobette

Untrusted Zone



Tenets of Zero Trust

(per NIST document)

1. All data sources and computing services are resources.
2. All communication is secured regardless of location.
3. Access to resources is granted on per-session basis.
4. Access to resources determined by dynamic policy.
5. Enterprise monitors integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced.
7. Enterprise collects as much info as possible about current state of system to improve security posture.

ZTA

(Proposed as a solution)

- **ZTA was proposed by Kindervag in 2010.**
- **Basic Assumptions [7]:**
  - The networks is in a dangerous environment all the time.
  - There are external or internal threats in the network from beginning to end
  - The location of the network is not enough to determine the credibility of the network
  - All devices, users, and network traffic should be authenticated and authorized.
  - Security policies must be dynamic and calculated based on as many data sources as possible.
- **Basic Principles [7]:**
  - Authenticate Users based on location, device, and behavior
  - Authenticate Devices and implement access control policies based on device identity and security
  - Restrict access and permissions: RBAC with the least privilege for the minimum time necessary to complete task
  - Adaptive: context-sensitive access policies that adapt continuously while informed by machine learning of contextual relationships

ZTA vs. RM vs. RVM

Reference Monitor (RM)

"An access control concept of an abstract machine that mediates all accesses to objects by subjects" [4].

Reference Validation Mechanism (RVM)

"An implementation of the reference monitor concept. An RVM must be tamperproof, must always be invoked (and can never be bypassed), and must be small enough to be subject to analysis and testing, the completeness of which can be assured" [4].

Follows NEAT acronym

- Non-bypassible
- Evaluable (e.g. verifiable)
- Always Invoked
- Tamper-proof

Zero-Trust Architecture (ZTA)

"set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level."

Core Technologies:

- Identity Authentication
- Access Control
- Trust Assessment

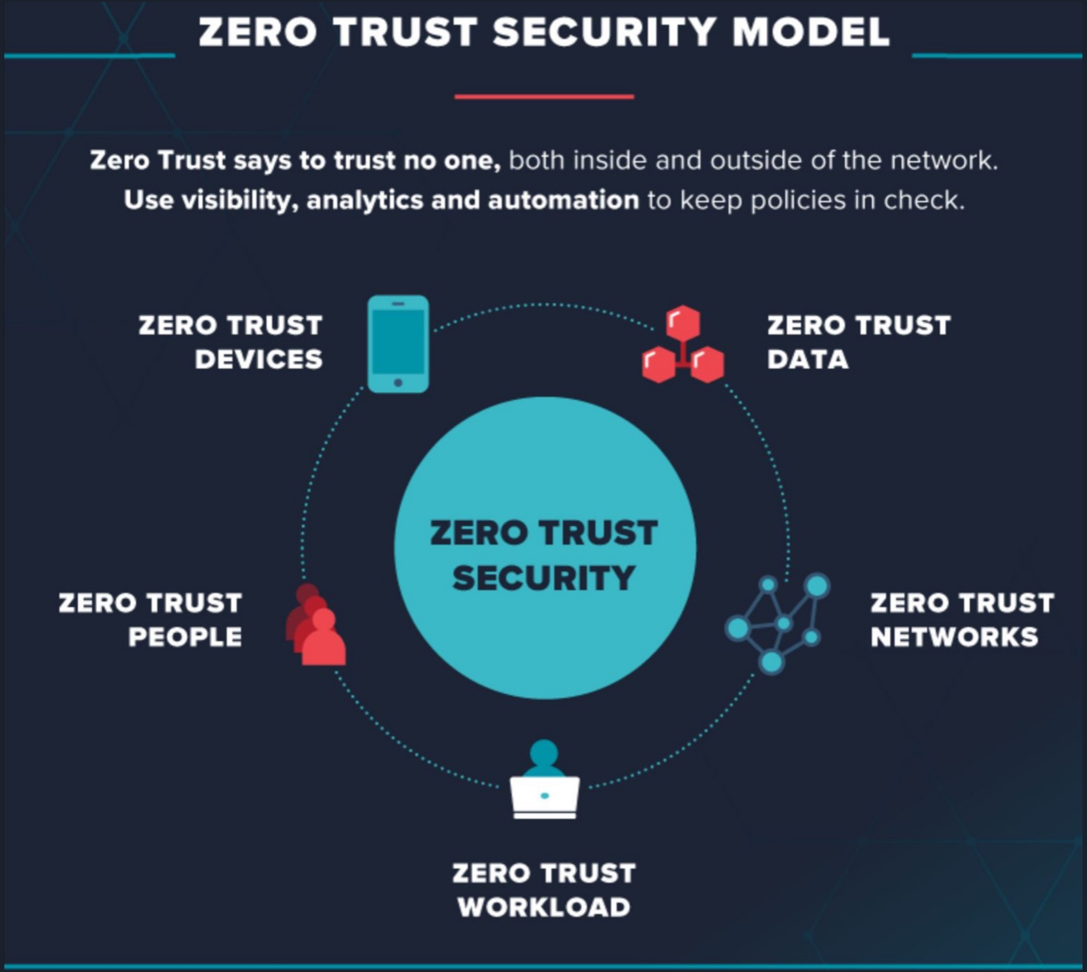

ZERO TRUST SECURITY MODEL
Zero Trust says to trust no one, both inside and outside of the network.
Use visibility, analytics and automation to keep policies in check.
ZERO TRUST DEVICES
ZERO TRUST DATA
ZERO TRUST SECURITY
ZERO TRUST PEOPLE
ZERO TRUST NETWORKS
ZERO TRUST WORKLOAD

Figure 1. Zero Trust Architecture Trust Concept [6].

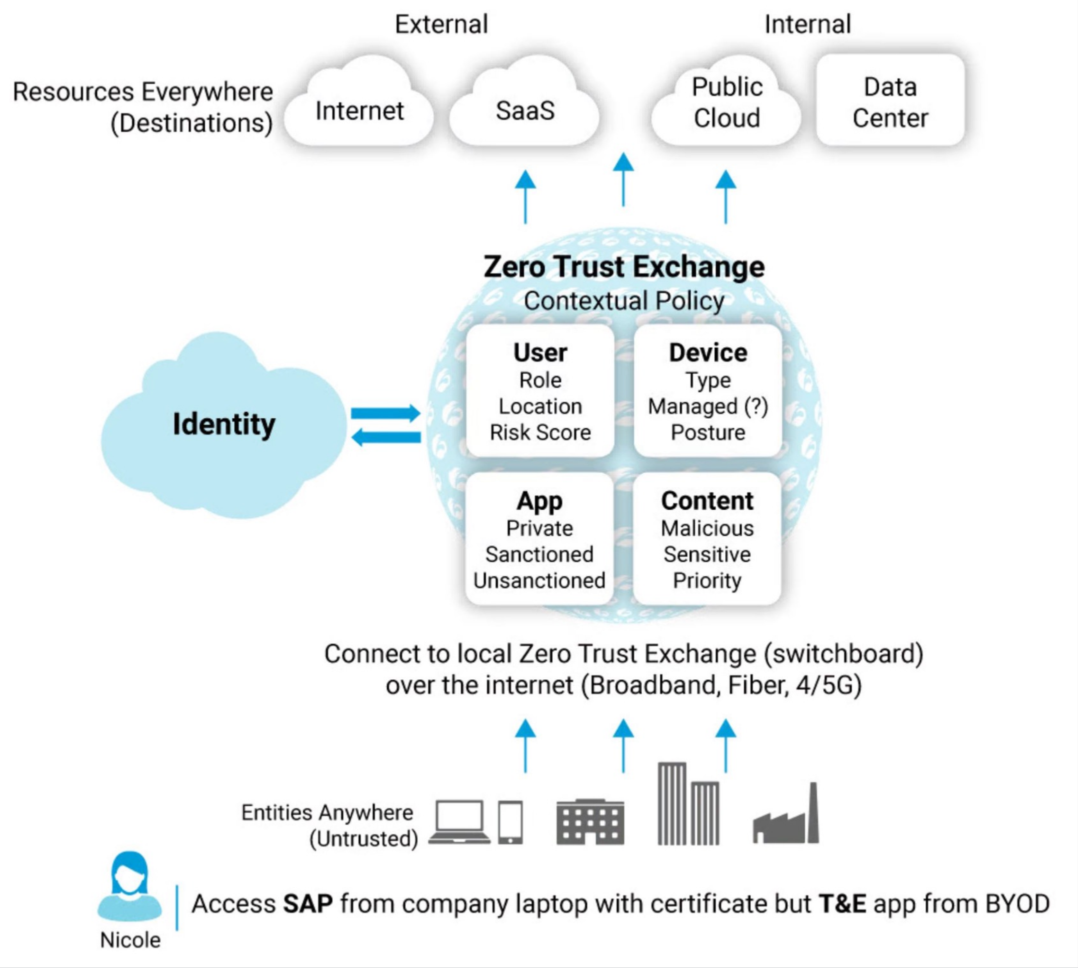

External
Internal
Resources Everywhere (Destinations)
Internet
SaaS
Public Cloud
Data Center
Zero Trust Exchange
Contextual Policy
Identity
User
Role
Location
Risk Score
Device
Type
Managed (?)
Posture
App
Private
Sanctioned
Unsanctioned
Content
Malicious
Sensitive
Priority
Connect to local Zero Trust Exchange (switchboard) over the internet (Broadband, Fiber, 4/5G)
Entities Anywhere (Untrusted)
Nicole
Access **SAP** from company laptop with certificate but **T&E** app from BYOD

Figure 2. Zero Trust Architecture Exchange Example [5].

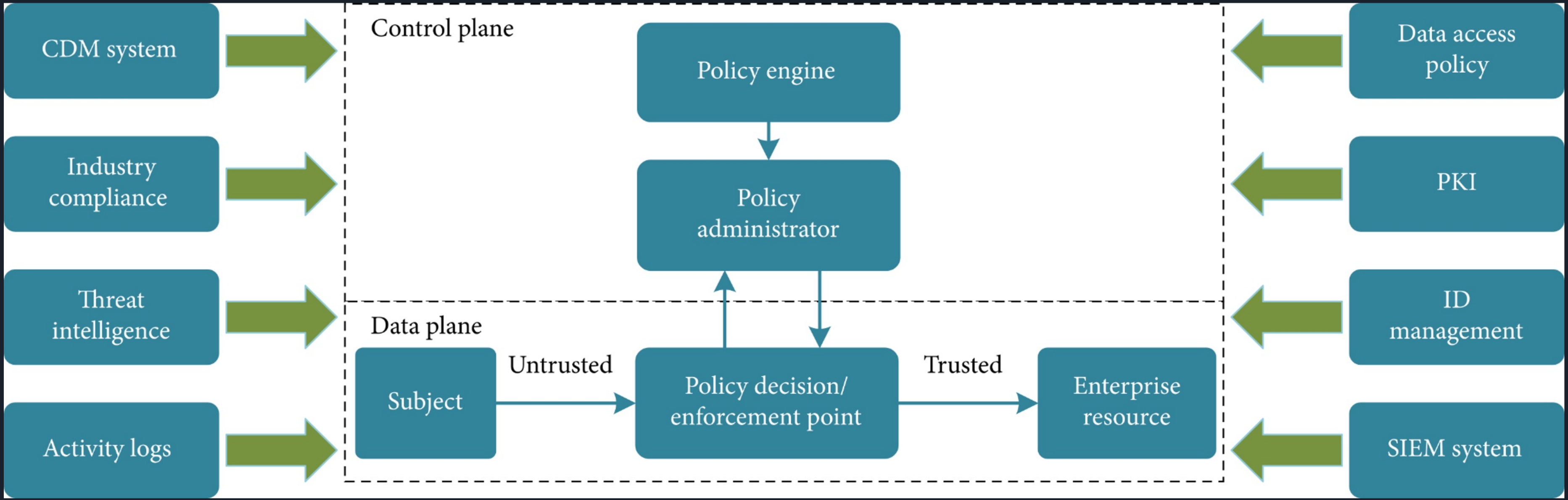


Figure 3. NIST example of ZTA [7].

General Advantages

- **Terminate every connection:**
  - All communications are denied from communicating until they are verified by their identity attributes.
  - Identity attributes are immutable properties that meet trust principles such as organization authentication and authorization policy requirements.
  - ZTA inspects all traffic in real time before it reaches the destination, effectively preventing ransomware, malware, and other malicious code [5].
  - This differs from firewalls that inspect files as they are delivered, delivering alerts that are often too late.
- **Reduce Attack Surface:**
  - ZTNA allows user connections directly to apps and resources they need, not the full network [5].
  - User-to-app and app-to-app connections eliminate a risk of lateral movement and the spread of infection.
  - Users and applications are invisible to public facing internet, so they can't be discovered or directly attacked.
- **Granular context-based policies:**
  - Access requests and rights are verified based on context, device, identity, location, content or application requested.
  - Access privileges are continually being reassessed as the context changes in real-time.

General Limitations

- **Increased time and effort during setup:**
  - Interconnection of all devices, users, applications, content and networks presents a greater development complexity and by result time cost.
  - Reorganization of existing business models to a ZTA may require complete overhaul depending on compatibility of legacy systems.
- **Increased Complexity:**
  - More users, applications, devices, content, and networks to manage and provide real-time identity verification based on context of communications
- **Increased ongoing user and application management requirements:**
  - Groups, Users, and access policies,
  - Application policies,
  - All must be closely monitored based on the real-time context based access decisions and tailored to specific user needs.
  - Access must be monitored for ongoing reassessment based on context.

References

[1] A. Kerman, “Zero trust cybersecurity: 'never trust, always verify',” *NIST*, 09-Nov-2021. [Online]. Available: https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify. [Accessed: 15-Oct-2022].

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “NIST SP 800-207: Zero trust architecture,” *CSRC*, 11-Aug-2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final. [Accessed: 15-Oct-2022].

[3] A. Irei, “7 steps for Implementing Zero Trust, with real-life examples,” *SearchSecurity*, 12-Oct-2022. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/How-to-implement-zero-trust-security-from-people-who-did-it. [Accessed: 15-Oct-2022].

[4] M. Bishop, E. Sullivan, and M. Ruppel, “Chapter 19,” in *Computer security: Art and science*, Boston: Addison-Wesley, 2019, pp. 512–512.

[5] “What is Zero trust? top benefits & how it works,” *Zscaler*. [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust. [Accessed: 15-Oct-2022].

[6] K. K. Tucker, “Pros and cons of the Zero trust model,” Infused Innovations, 22-Jul-2021. [Online]. Available: https://www.infusedinnovations.com/blog/secure-intelligent-workplace/pros-and-cons-of-the-zero-trust-model. [Accessed: 15-Oct-2022].

[7] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends", *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6476274, 13 pages, 2022. https://doi.org/10.1155/2022/6476274