Zero Trust Architecture

The Seven Tenets of Zero Trust

Abstract

Forrester Research has said "Zero Trust is becoming the security model of choice for enterprises and governments alike." If your CIO or CISO asked you to develop a ZTA plan for your mainframe would you know where to start? This Webinar will show you the seven tenets of Zero Trust, and why they are important. After this presentation, you will know what ZTA is and what it means for your mainframe.

About the Presenter

Charles has been writing mainframe software for longer than he cares to admit. He developed security software for eight years at CorreLog, where he authored the zDefender and SyslogDefender products which were acquired by BMC.

Agenda

Why should I care about ZTA?

What are Zero Trust and ZTA?

- The Seven Tenets of Zero Trust
- Zero Trust Architecture

Problems with ZTA

What can you do?

- A mainframe action plan

National Institute of Standards and Technology (NIST)

"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)."

– NIST SP 800-207
"Zero Trust Architecture"
August, 2020

Forrester Research

"Zero Trust is becoming the security model of choice for enterprises and governments alike. However, security leaders often don't know where to begin to implement it, or they feel daunted by the fundamental shifts in strategy and architecture Zero Trust demands. However, Zero Trust does not require that you rip out all your current security controls to start fresh, and with the right approach you can realize benefits right away. "

– Forrester Research, Inc., report RES157736

Zero Trust in the news

"The Ransomware Crime Wave Has Made Zero Trust Critical"

- eWeek.com, July 12, 2021

"How to prevent ransomware attacks with a zero-trust security model"

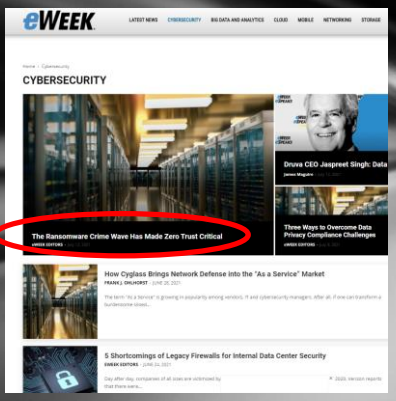
- TechRepublic, July 9, 2021

"CISA Collaborating With White House on Forthcoming Zero-Trust Strategy"

- Nextgov.com, June 22, 2021

"GSA stresses agencies align IPv6 and zero-trust plans ahead of next week's deadline"

- Fedscoop.com, July 13, 2021



So why should you care?

One of these days your CIO or CISO is going to announce a ZTA initiative …

Or perhaps he or she already has

What does it mean?

What does it mean for z/OS?

What are you going to do?

What are Zero Trust and ZTA?

My definition

A major de-emphasis on perimeter security. A terminal or a user is not trusted simply because he or she is inside the firewall or similar. Encryption of internal traffic just like external.

- Perhaps there is no such thing as a perimeter?

A de-emphasis on trusted devices and trusted people. All security is transaction by transaction, or at least by some small window in time.

Security is granular, not all or nothing. It is not that Bob is "trusted" – it is that he is authorized (or not) to do some particular transaction.

A lot less trust …

Formal Definitions (from NIST SP 800-207)

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

ZTA History

Defense Information Systems Agency (DISA) "BCORE" advocated moving from perimeter to transaction security

Jericho Forum, 2004. Defined and promoted "de-perimeterisation"

- Limiting implicit trust based on network location and/or single static defenses

Term "Zero Trust" popularized by John Kindervag of Forrester Research

- Term actually coined in 1994 by Stephen Paul Marsh in a doctoral thesis on social trust

NIST SP 800-207, 2020. Popularized the term and the concept, especially in the Federal government

BeyondCorp: Zero Trust at Google

In 2010 Google disclosed the only known hack of Google intellectual property, "Operation Aurora"

- "Elderwood Group" with ties to China People's Liberation Army
- Goal of compromising source code in SCMs

Discovered dozens of other companies had also been breached by Aurora

- Adobe, Akamai, Juniper, Rackspace, …

In response Google re-thought their entire approach to security

Moved from perimeter defense (firewalls, VPNs) to per-request authorizations

Google dubbed their approach BeyondCorp

Now available as a Google Cloud service

Zero Trust is also known as

The zero trust security model

Zero trust network architecture

ZTNA

Perimeterless security

Before ZTA – Perimeter Security

Perimeter defenses

Firewalls

VPNs

DMZs

Border routers

Packet filters

IDs and Passwords

Screened subnets

Once inside perimeter users are trusted

What could possibly go wrong?

Malicious Actors from Inside the Perimeter

Insider threats

- "More than 30% of breaches in 2019 were the work of insiders" – Verizon 2020 Data Breach Investigations Report

Phishing makes outsiders appear to be insiders

July 2020 Twitter employees working from home victims of voice phishing (vishing) – hackers impersonated and changed passwords of Barack Obama, Joe Biden, Kanye West …

Terminated employees with employee credentials

Source: Wikimedia

Perimeter less and less well-defined

Cloud computing

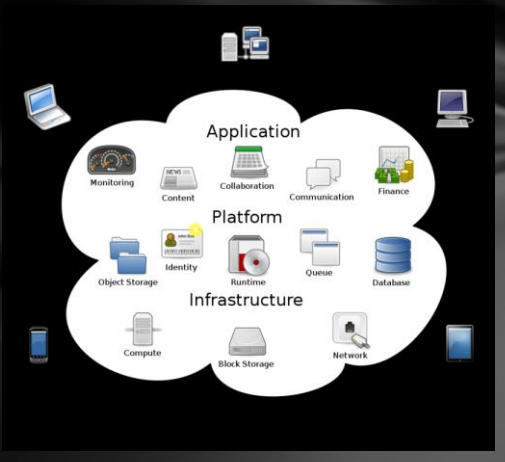
Partner companies

Bring your own device

Work from home

Where is the perimeter anyway?

Time for a new paradigm…



Source: Wikipedia. Created by Sam Johnson

ZTA: Trust No One

Trust no one?

- Used to trust everyone inside the perimeter
- Now told to trust no one
- Oh-oh!
- What to do?

Well, not exactly "no one," of course

"Trust, but verify"

Authenticate user's identity

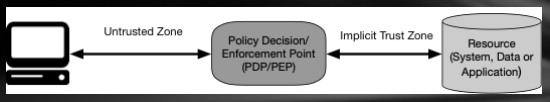
Validate user's device's security posture

Consider time of day, location, etc.

Then admit user to an "implicit trust zone"

But admission to implicit trust zone does not imply complete trust

Airport security model: you go through security and are admitted to waiting areas, etc. – but not the tarmac or control tower



Source: NIST SP 800-207

The Seven Tenets of Zero Trust

Per NIST 800-207 Zero Trust Architecture

The Seven Tenets of Zero Trust

1. All data sources and services are considered resources
   - Network may be composed of multiple classes of devices
     - Small footprint devices
     - Software-as-a-Service Systems
     - Personally-owned devices
     - They are all resources
   - Is a mobile phone a user or a resource? Yes.

The Seven Tenets of Zero Trust

2. All communication is secured regardless of network location
   - Access from inside perimeter treated the same as external access
   - Trust not automatically granted based on inside-the-perimeter location
   - All communication – internal and external – should be secure

The Seven Tenets of Zero Trust

3. Access to enterprise resources is granted on per-session basis
   - Trust in the requester is evaluated before the access is granted
   - Could mean "sometime recently" and not directly before transaction
   - Access granted with the least privileges needed
   - Authorization to one resource does not grant access to different resource

The Seven Tenets of Zero Trust

4. **Access to resources is determined by dynamic policy**
   - Observable state of client identity
     - May include additional attributes besides user ID
     - Behavioral attributes including analytics and deviations from normal usage patterns
   - Application or servicer requesting access
     - Asset state may include software versions, date/time, etc.
   - Other behavioral or environmental attributes
   - May vary based on sensitivity of the resource
   - Least privilege principles

The Seven Tenets of Zero Trust

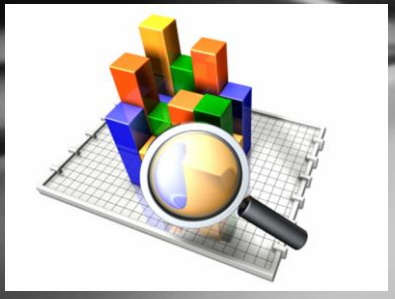
5. **Enterprise monitors and measures the integrity and security posture of all assets**
   - No asset is inherently trusted
   - Continuous monitoring of state of devices and applications
   - Discovery of compromised assets
   - Applies to personally-owned devices as well as enterprise devices

The Seven Tenets of Zero Trust

6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed**
   - Constant cycle of obtaining access, scanning and assessing threats, adapting, and reevaluating trust
   - Identity, Credential, and Access Management (ICAM) and asset management systems a prerequisite to ZTA
   - Multifactor authentication (MFA) for access to some or all enterprise resources
   - Continual monitoring with possible re-authentication and reauthorization throughout user transactions

The Seven Tenets of Zero Trust

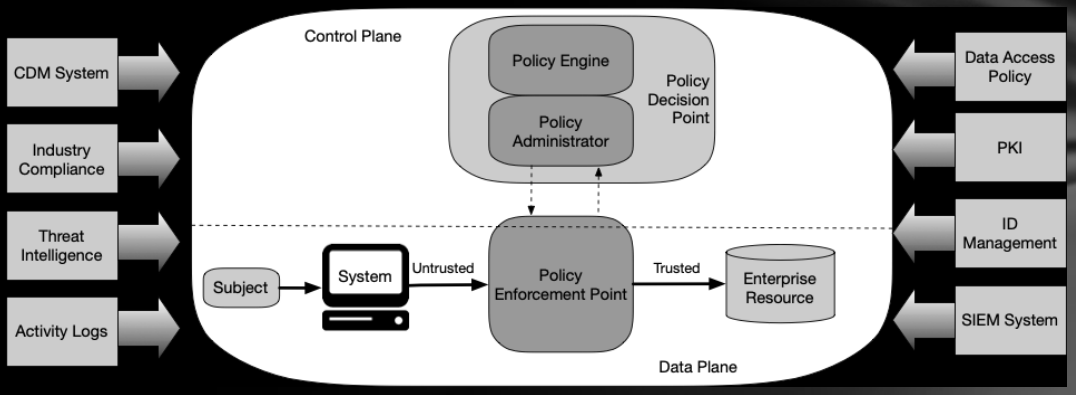
7. **Enterprise collects as much information as possible about current state of assets, network infrastructure and communications and uses it to improve security posture**
   - **Security posture, network traffic and access requests**
   - **Same data can also be used for access request context**



Logical Components of ZTA

Per NIST 800-207 Zero Trust Architecture

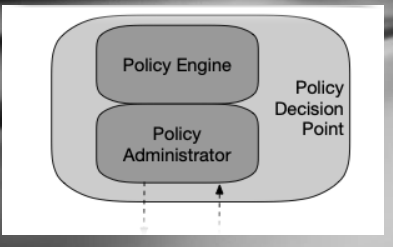
Logical Components of ZTA



Source: NIST SP 800-207

Policy Engine (PE)

- Responsible for the ultimate decision to grant, deny or revoke access to a resource for a given subject.
- PE uses enterprise policy and input from external sources (e.g., CDM systems, threat intelligence services) as input to a trust algorithm
- PE is paired with the policy administrator component.
- PE makes and logs the decision
- Policy administrator executes the decision



Policy Administrator (PA)

Responsible for establishing and/or shutting down communication path between subject and resource

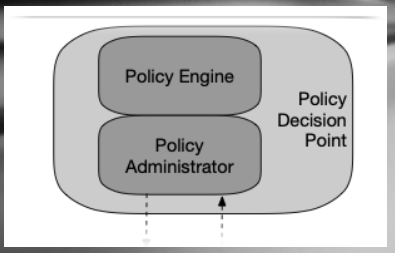
Does so via commands to Policy Enforcement Points (PEPs)

Generates any session-specific authentication and authentication token or credential for access to a resource.

If access authorized configures the Policy Enforcement Point (PEP) to allow the session

If session is denied PA signals to PEP to shut down the connection.

Closely tied to the PE. Some implementations may treat the PE and PA as a single service



Policy Enforcement Point (PEP)

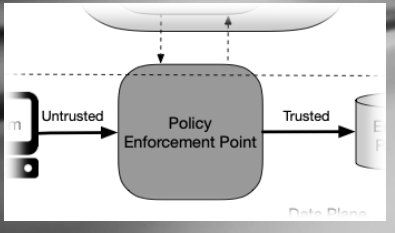
Responsible for enabling, monitoring, and terminating connections between subject and resource

PEP communicates with PA to forward requests and/or receive policy updates from PA

PEP is a single logical component in ZTA but may be implemented as single component or two different components:

- Client side (e.g., agent on a laptop)
- Resource side (e.g., gateway component in front of resource)

Beyond the PEP is the trust zone hosting the resource



Inputs to the Policy Components

Continuous diagnostics and mitigation (CDM) system:

- Gathers information about the enterprise asset's current state and applies updates to configuration and software components
- Provides policy engine with information about the asset making an access request, such as whether it is running an appropriately patched OS, or whether it is a non-enterprise device

Industry compliance system:

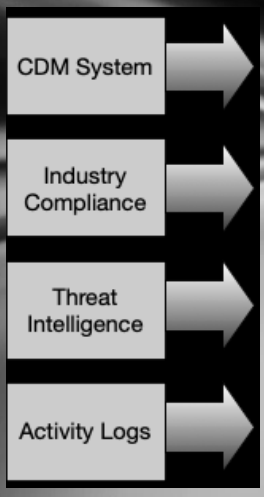
- Ensures that the enterprise remains compliant with any relevant regulatory regime (FISMA, HIPAA, PCI DSS, etc.)

Threat intelligence feed(s):

- Provides information from internal or external sources that provide information about attacks or vulnerabilities (newly discovered flaws in software, newly identified malware, reported attacks to other assets, etc.)

Network and system activity logs:

- Aggregates asset logs, network traffic, resource access actions, and other events that provide feedback on security posture of enterprise information systems



Additional Inputs to the Policy Components

Data access policies:

- Attributes, rules, and policies about access to enterprise resources
- Could be encoded by management or dynamically generated by policy engine
- Starting point for authorizing access to a resource
- Should be based on the defined mission and roles of the organization

Enterprise public key infrastructure (PKI):

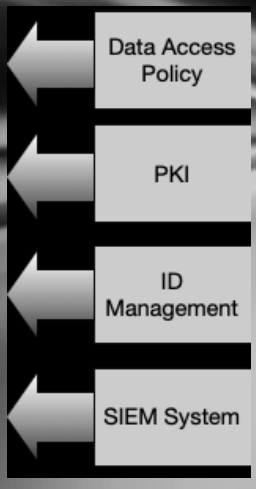
- Responsible for X.509 certificates

ID management system:

- Responsible for managing enterprise user accounts
- Could be a lightweight directory access protocol (LDAP) server
- Might include non-enterprise users and assets

Security information and event management (SIEM) system:

- Collects security-centric information for later analysis
- Data is used to refine policies and/or warn of possible attacks



Trust Algorithm (in Policy Engine)

Access request: actual request from the subject.

- Resource requested is the primary information
- Information about the requester, such as OS version, software (does application appear on approved list?), and patch level

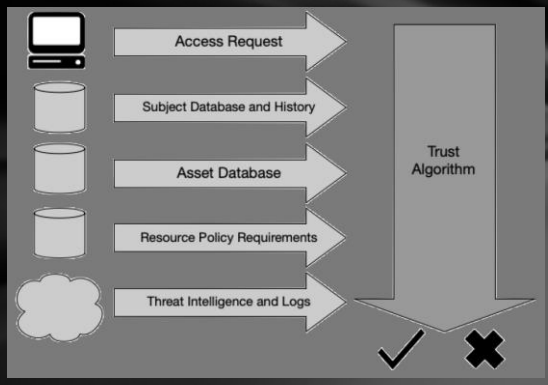
Subject database: The "who" that is requesting access to a resource

Asset database: Contains the known status of each enterprise (and possibly non-enterprise/BYOD) asset

Resource requirements: defines minimal requirements for access to the resource

- Might include authenticator assurance levels, such as MFA network location (e.g., deny access from overseas IP addresses), data sensitivity, etc.

Threat intelligence: Information feed about general threats and active malware



"The policy engine can be thought of as the brain and the trust algorithm as its primary thought process "

Is ZTA Perfect?

Threats Associated with ZTA

Subversion of the Policy Decision (PE & PA) process

- Administrator error or malice

Denial-of-Service or similar Network Disruption

- Botnet DDOS against Cloud PE/PA provider?

Stolen Credentials/Insider Threats

- Phishing attacks
- Malicious insiders
- At least ZTA limits scope of exposure

Integrity of Access Policy Database

Each asset has own security parameters, complicating replacement

Risks from use of automated technology for security decisions

User Impacts from ZTA

Not known – lack of ZTA implementations

User reactions to MFA a good analog

- "Security Fatigue" if security is intrusive and impacts productivity
- Good acceptance if streamlined
- Resentment if feeling of constant monitoring for violations

What Can You Do?

Good News is Mainframe is Mostly There

We have had role-based security for years

Security based on specific permissions, not all-or-nothing trust

- But static, "legacy" PERMITs not exactly Zero Trust

The mainframe had its security epiphany in 1975 or so

- The rest of the IT world discovered security somewhere around 1986

The future is likely to be different

- Mainframe has had a string of pretty good security luck
- Mainframe likely to become a primary intrusion target
- "I rob banks because that's where the money is" – Willie Sutton

Your Mainframe and ZTA

If you rely on perimeter security then mainframe only as secure as Windows or partner systems network

- "Lateral movement"
- It's not "treat internal networks as secure; external networks as insecure" – it's "treat all networks as insecure."
- Don't trust a transaction just because it came from "your" network
- Target* breach: attackers came in through partner vendor network, and once "in" were in

There is no single provider of a comprehensive mainframe ZTA solution

*Not a mainframe breach

A Mainframe Action Plan

Pervasive encryption

- NIST calls for "encrypting all [network] traffic"

Some mainframe "all-or-nothing" trust to consider

- APF Authorization
  - Move toward FACILITY class permissions instead
  - Question ISV requirements for APF
- RACF SPECIAL and OPERATIONS and UID zero and BPX.SUPERUSER
  - Don't use as a lazy substitute for well-thought-out PERMITs
- UACC and ID(*)

NIST says attackers will focus on processes that have not had ZTA applied — will target the low-hanging fruit

- Don't let your mainframe be the low-hanging fruit

NewEra Multi-Factor Edit (MFE)

An example of a practical ZTA implementation step

ZTA says access rules must be as granular as possible

Traditional PERMITs at data set level

- No member-level granularity in RACF
- PARMLIBs and PROCLIBs – all or nothing access

MFE provides member and UNIX file "categories"

Restrict categories of configuration to specific USERIDs

Enhanced access requirements by category

- MFA, one-time-use tokens, etc.

Also Journaling, Audit, Backup, Restore and Reporting

CONTROL EDITOR

Questions?

More questions?
charlesm@mcn.org

Summary

Why you should care about ZTA

What are Zero Trust and ZTA?

- The Seven Tenets of Zero Trust
- Zero Trust Architecture

Problems with ZTA

What can you do?

- An action plan for your mainframe

Acknowledgements and References

NIST Special Publication 800-207 Zero Trust Architecture

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- This presentation is largely based on NIST SP 800-207. Most otherwise uncredited illustrations are from this publication.

BEYONDCORP: A NEW APPROACH TO ENTERPRISE SECURITY [at Google]

- https://www.usenix.org/publications/login/dec14/ward

Build Security Into Your Network's DNA: The Zero Trust Network Architecture ($745)

- https://www.forrester.com/report/Build+Security+Into+Your+Networks+DNA+The+Zero+Trust+Network+Architecture/-/E-RES57047

A Practical Guide To A Zero Trust Implementation

- https://reprints.forrester.com/#/assets/2/53/RES157736/reports

Developing a Framework to Improve Critical Infrastructure Cybersecurity [links to Forrester papers]

- https://www.nist.gov/system/files/documents/2017/06/05/040813_forrester_research.pdf

Google: A new approach to China

- https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Thank you

More questions? Comments?
charlesm@mcn.org