Zero Trust for Supply Chain Security

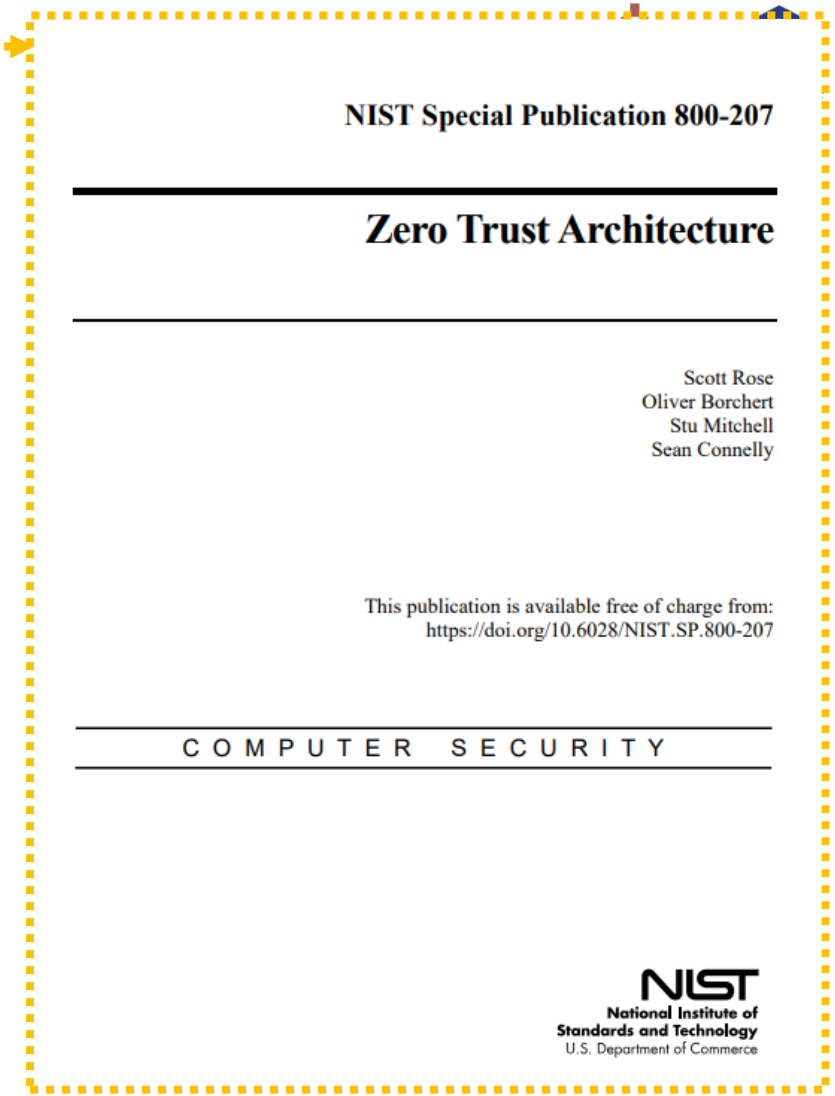
Hannam University
Manhee Lee

Contents

- NIST 800-207 Zero Trust Architecture
- Executive Order 14028
    - Critical Software Security Measure
    - Secure Software Development Framework(SSDF)
- ZT for Critical Software Security Measure
- ZT for SSDF

NIST 800-207 Zero Trust Architecture

- In 2018, the ZTA document released by NIST
  - Currently being used as a reference in various ZTA models.
- Contents
  - Zero Trust Basics
  - Logical Components of Zero Trust Architecture
  - Deployment Scenarios/Use Cases
  - Threats Associated with Zero Trust Architecture



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ZTA: Tenets of Zero Trust

1	All data sources and computing services are considered resources.
2	All communication is secured regardless of network location.
3	Access to individual enterprise resources is granted on a per-session basis.
4	Access to resources is determined by dynamic policy-including the observable state of client identity, application/service, and the requesting asset-and may include other behavioral and environmental attributes.
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Structure of EO-14028

Critical software

Definition, Category, Protection

SBOM Software Bill of Materials ntia.gov/sbom #SBOM

HANNAM 한남대학교

SOFTVERSE

Minimum Requirement

EXECUTIVE ORDER 14028

Minimum Verification Standard
Secure Software Development Framework

USDA

USAID FROM THE AMERICAN PEOPLE

OPIC

MILLENNIUM CHALLENGE CORPORATION

US Army Corps of Engineers

Cybersecurity Supply Chain Risk Management Practices

Definition, Category, Protection

Definition

- is designed to run with elevated privilege or manage privileges;
- has direct or privileged access to networking or computing resources;
- is designed to control access to data or operational technology;
- performs a function critical to trust; or,
- operates outside of normal trust boundaries with privileged access.

Definition, Category, Protection

Category

• Identity, credential, and access management (ICAM) • Operating systems, hypervisors, container environments • web browser • endpoint security • network control	• network protection • network monitoring & configuration • operational monitoring & analysis • remote scanning • remote access & configuration management • backup/recovery & remote storage

Critical software

Definition, Category, Protection

Objective	Security Measures
1	Protect EO-critical software and EO-critical software platforms from unauthorized access and usage
2	Protect the confidentiality, integrity, and availability of data used by EO-critical software and EO-critical software platforms.
3	Identify and maintain EO-critical software platforms and the software deployed to those platforms to protect the EO-critical software from exploitation.
4	Quickly detect, respond to, and recover from threats and incidents involving EO-critical software and EO-critical software platforms.
5	Strengthen the understanding and performance of humans' actions that foster the security of EO-critical software and EO-critical software platforms.

Definition, Category, Protection

Objective	Security Measures	NIST 800-207 Tenets of ZTA
1.1	Use multi-factor authentication that is verifier impersonation-resistant for all users and administrators of EO-critical software and EO-critical software platforms.	6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. -This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources.
1.2	Uniquely identify and authenticate each service attempting to access EO-critical software or EO-critical software platforms.	3. Access to individual enterprise resources is granted on a per-session basis.
1.3	Follow privileged access management principles for network-based administration of EO-critical software and EO-critical software platforms.	3. Access to individual enterprise resources is granted on a per-session basis. -Access should also be granted with the least privileges needed to complete the task.
1.4	Employ boundary protection techniques as appropriate to minimize direct access	6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

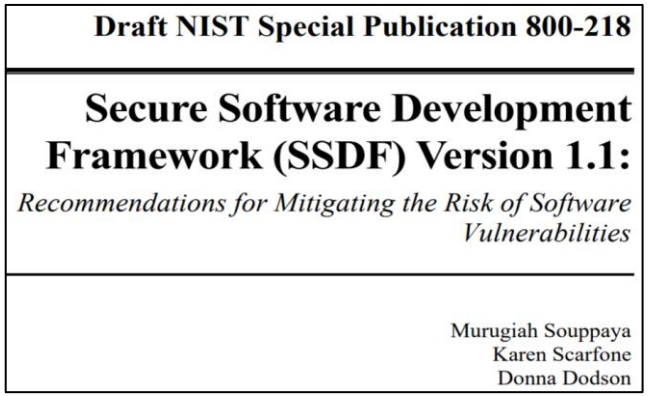
Definition, Category, Protection

Objective 1	Security Measures	NIST 800-207 Tenets of ZTA
2.2	Use fine-grained access control for data and resources used by EO-critical software and EO-critical software platforms to enforce the principle of least privilege to the extent possible.	3. Access to individual enterprise resources is granted on a per-session basis. -Access should also be granted with the least privileges needed to complete the task.
2.4	Protect data in transit by using mutual authentication whenever feasible and by encrypting sensitive data communications	2. All communication is secured regardless of network location. -All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source Authentication
4.1	Configure logging to record the necessary information about security events involving EO-critical software platforms and all software running on those platforms.	7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.
4.2	Continuously monitor the security of EO-critical software platforms and all software running on those platforms.	

SSDF(Secure Software Development Framework)

◆ NIST SP 800-218

Practices	Explanations
1. Prepare the Organization (PO)	Ensure that the organization's people, processes, and technology are prepared to perform secure software development at the organization level and, in some cases, for individual development groups or projects.
2. Protect the Software (PS)	Protect all components of the software from tampering and unauthorized access.
3. Produce Well-Secured Software (PW)	Produce well-secured software with minimal security vulnerabilities in its releases.
4. Respond to Vulnerabilities (RV)	Identify residual vulnerabilities in software releases and respond appropriately to address those vulnerabilities and prevent similar vulnerabilities from occurring in the future.


Draft NIST Special Publication 800-218

Secure Software Development Framework (SSDF) Version 1.1:

Recommendations for Mitigating the Risk of Software Vulnerabilities

Murugiah Souppaya
Karen Scarfone
Donna Dodson

SSDF and Zero Trust

Practices	NIST 800-207 Tasks and Examples	NIST 800-207 Tenets of ZTA
PO 5.1	**Separate and protect each environment involved in software development.** -Example 1: **Use multi-factor, risk-based authentication** and conditional access for each environment. -Example 3: Enforce authentication and tightly restrict connections entering and exiting each software development environment, including **minimizing access to the internet to only what is necessary.**	6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. -This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. 3. Access to individual enterprise resources is granted on a per-session basis. -Access should also be granted with the least privileges needed to complete the task.
PO.5.2	**Secure and harden development endpoints** (i.e., endpoints for software designers, developers, testers, builders, etc.) to perform development-related tasks using a risk-based approach. -Example 3: **Continuously monitor the security posture** of all development endpoints, including monitoring and auditing all use of privileged access. -Example 5: **Require multi-factor authentication for all access to development endpoints and development resources.** -Example 7: **Configure each development endpoint following a zero trust architecture.**	6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. -This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. 7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

SSDF and Zero Trust

Practices	NIST 800-207 Tasks and Examples	NIST 800-207 Tenets of ZTA
PS 1.1	Store all forms of code – including source code, executable code, and configuration-as-code – based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access.	3. Access to individual enterprise resources is granted on a per-session basis. -Access should also be granted with the least privileges needed to complete the task.
PS.3.1	Securely archive the necessary files and supporting data (e.g., integrity verification information, provenance data) to be retained for each software release. -Example 1: Store the release files, associated images, etc. in repositories following the organization's established policy. Allow read-only access to them by necessary personnel and no access by anyone else.	6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. -This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. 7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Conclusion

- Self-Attestation will be mandated by U.S. federal agencies
  - Affect SW development practices for public and private sector
  - Change security and compliance requirements for exporting to U.S.
- Zero Trust is key functions for Critical SW security measures and SSDF

Zero Trust necessary for better supply chain security!!