Zero Trust Architecture

Understanding the Core Principles and Implementation

Rajendra Hegadi, IIIT Dharwad

Introduction to Zero Trust Architecture

1. Zero Trust Architecture (ZTA) is a cybersecurity model based on the principle of 'never trust, always verify.'
2. It assumes that threats can exist both inside and outside the network, and therefore, every access request must be authenticated and authorized.

Introduction to Zero Trust Architecture

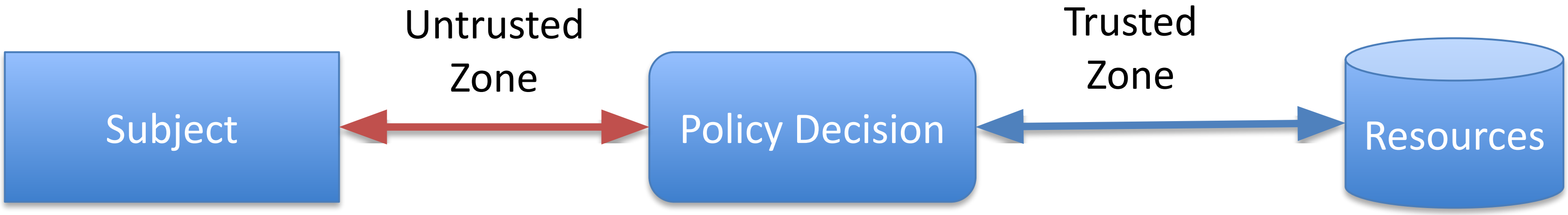
- Resource protection and the Idea is that trust is never granted implicitly but must be continually evaluated
- It is an end-to-end approach to enterprise resource and data security that encompasses identity (person and non-person entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.

Key Principles of Zero Trust Architecture

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.

1. Verify Explicitly
2. Use Least Privilege Access
3. Assume Breach

ZTA- Access Model



Subject

Untrusted Zone

Policy Decision

Trusted Zone

Resources

Application, Device
Person etc

Policy decision point (PDP)
policy enforcement point (PEP)

System, Data,
Applications

- Zero trust applies to two basic areas: *authentication* and *authorization*.
- Implicit trust zone must be as small as possible
- Example airport

ZTA- Level of confidence - Dynamic Risk based Policies

- What is the level of confidence about the subject’s identity for this unique request?
- Is access to the resource allowable given the level of confidence in the subject’s identity?
- Does the device used for the request have the proper security posture?
- Are there other factors that should be considered and that change the confidence level (e.g., time, location of subject, subject’s security posture)?

Core Components of Zero Trust Architecture

1. Identity and Access Management (IAM)
2. Device Security
3. Network Segmentation
4. Continuous Monitoring and Analytics
5. Data Protection
6. Automation and Orchestration

Benefits of Zero Trust Architecture

1. Reduced Risk
2. Enhanced Compliance
3. Scalability

Challenges in Implementing Zero Trust

1. Complexity
2. Cost
3. Cultural Resistance

Conclusion

- Zero Trust Architecture is a comprehensive approach to modern cybersecurity.
- By continuously verifying trust, enforcing least privilege access, and assuming breach, organizations can better protect their assets in an increasingly complex threat landscape.

References

- Zero Trust Architecture, NIST Special Publication 800-207

https://doi.org/10.6028/NIST.SP.800-207