Zero Trust Discussion

December 17, 2020

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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.

DM20-1178

Seven Basic Tenets for Zero Trust (ZT)

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.

Current Takeaways of ZT Research - 1

ZT is an accumulation of architecture patterns, not a product.

DoD historically uses perimeter security model. This approach fails with cloud, IoT, mobile, BYOD, remote workforces, and requires moving security to the service (i.e., Kubernetes, DevSecOps, …).

ZT requires authentication, authorization, monitoring, detection, and response to the service level, inferring automation and accurate asset management to scale.

DoD will not be able to “purchase ZT” because DoD systems are continuously evolving systems-of-systems (SoS)s that leverage agile frameworks and no longer have technical “perimeters” (Platform One, Cloud One, DSOP).

Current Takeaways of ZT Research - 2

Agile and ZT require organizations to change how they operate and ZT needs to be the baseline.

ZT is a strategic goal, not a final destination, and requires appropriate measurement to understand current state and course correction.

ZT must be part of the organizational culture and requires ongoing commitment at the C-level.

Approach to Investigating ZT

1. Model of system transitioning services to cloud service provider (CSP).
2. Technical research of ZT technologies and telemetry information.
3. Reference implementation and transition guidance.
4. ZT cybersecurity situational awareness.

Outcomes and Impacts

Digital engineering model used for ZTA design, tradeoffs, and implementation analysis for DoD enterprises/weapon systems.

Security assessment approach for early risk identification and support authority-to-operate requirements.

Transitionable guidance to improve organizations' ability to employ ZTA to improve security of enterprises/systems to spur community's adoption.

Model Based Systems Engineering

System Definition

Requirements Model

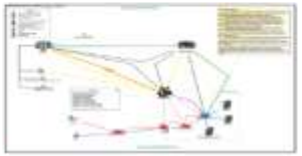
- Establish Source/Originating Requirements
- Structured Hierarchy and Flowdown
- Managed Traceability
  - Level I to Derived Requirements
  - Requirements to Simulation and Verification Elements

Allocated Architecture

Analysis Model

- Validate Performance
  - Requirements Model Update
- Functional Model Execution via Discrete Event Simulation
  - Timeline Analyses
  - Resource Analyses
  - Quantitative Benefits Analyses
  - Validation of Logic

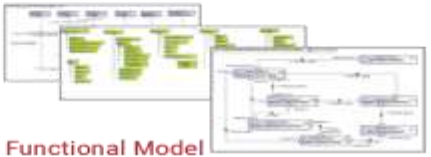
System Vision



System Model

- Concept of Operation
- End-to-end Mission Threads/Workflows
- Identification of System Qualities
- Roadmap Development

Functional Architecture



Functional Model

- Translate User Operational Capabilities to System Functional Requirements
- Graphical Analysis Provides Increased Rigor (vs text only)
  - Functions
  - Input/Output
  - Time Sequence
  - Logic
- Scenario Development
  - Operational
  - Simulation
  - System Qualities

Physical Architecture

Functional Model

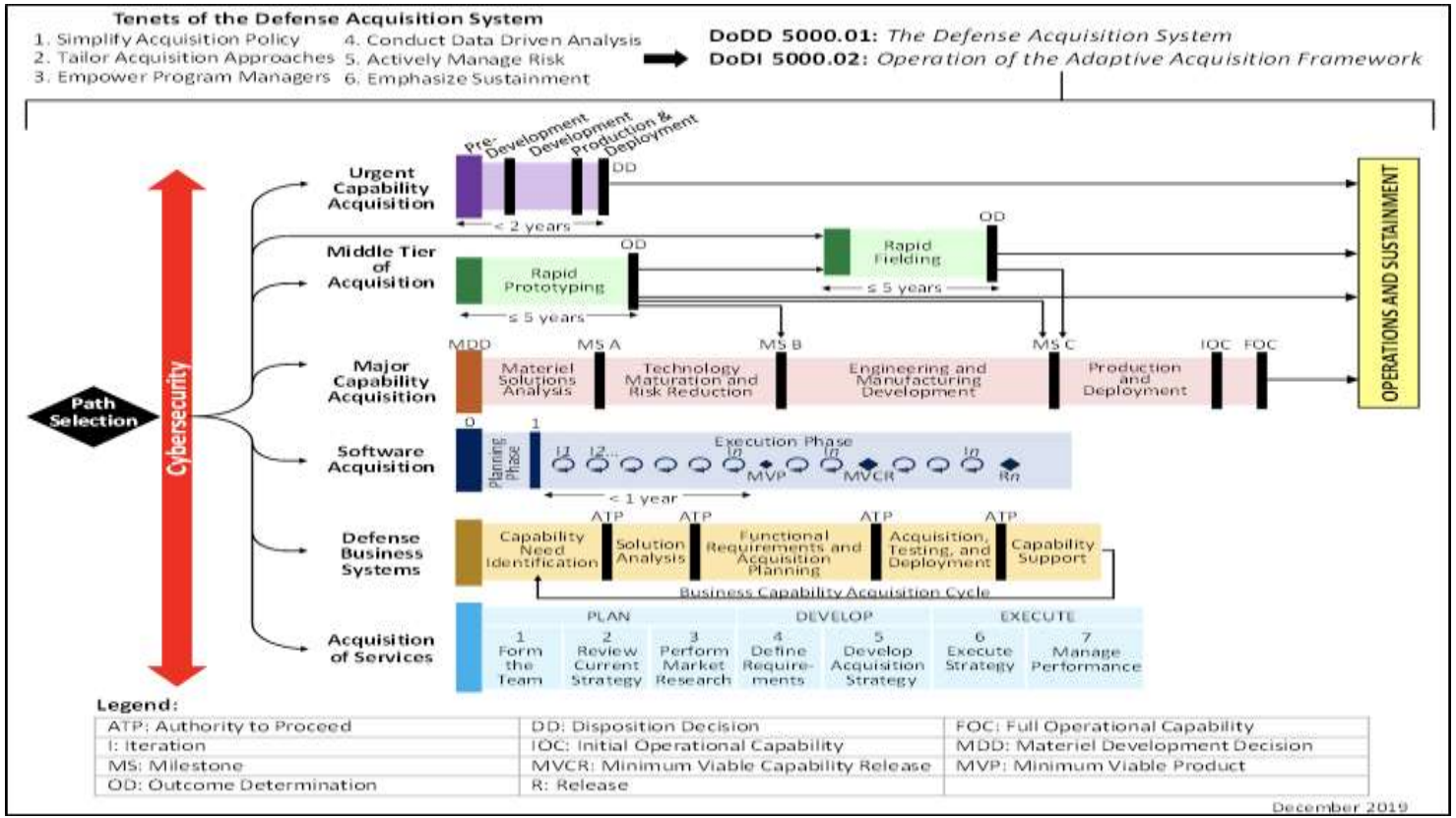
- Candidate Physical Architectures
  - HW, SW, Interfaces
  - Human Operators
- Allocate Functions to Components
- Platform Compatibility Assessments
- System Physical Architecture Definition

SoS, System, and Software Architecture

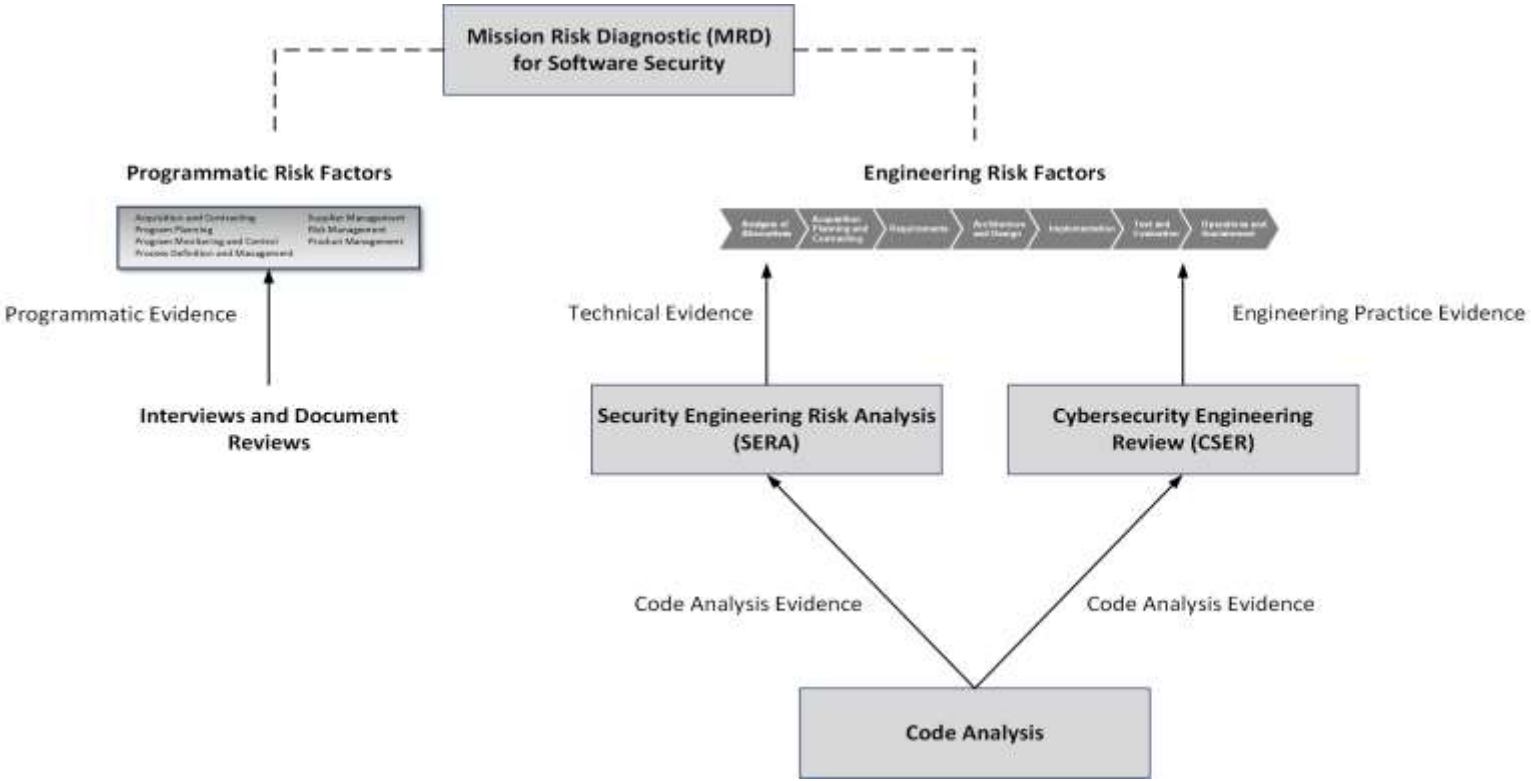
Need to develop documentation to support architecture analysis of the implementation, operation, and security of systems which operate in hybrid, multi-cloud, multiple security enclaves development, production, and test environments where Artificial Intelligence and Machine Learning (AI/ML) approaches/solutions can be applied in a digital engineering environment.

- Development of conceptual, capability, operational, systems/services, security, and stakeholder architecture views that will provide a vision for the system which include the conceptual, logical, and physical designs. (As-Is and To-Be architectures; operational, developmental, and lifecycle support mission threads and scenarios to help provide a vision for the systems to enhance concept of operations (CONOPs) development; mission-specific reference architectures for systems.
- Requirements development, consolidation, and refinement which includes gathering objectives and identifying mission, stakeholders, users, non-functional, and performance requirements.
- Business case and comparative analysis of capabilities and operational activities in support of transitioning to cloud services, AI/ML, and zero trust architecture.

Adaptive Acquisition Framework: *Multiple Acquisition Pathways*



Situational Awareness (SA) Cybersecurity Engineering (CSE) Assessments: *An Integrated View*



Mission Risk Diagnostic (MRD)

What

- An approach for assessing mission risk in interactively complex, socio-technical systems (e.g., acquisition programs, development projects, enterprise initiatives, organizational capabilities)

Why

- Assess a mission's current potential for success in relation to a set of known risk factors
- Develop a plan for managing risk and increasing the potential for mission success

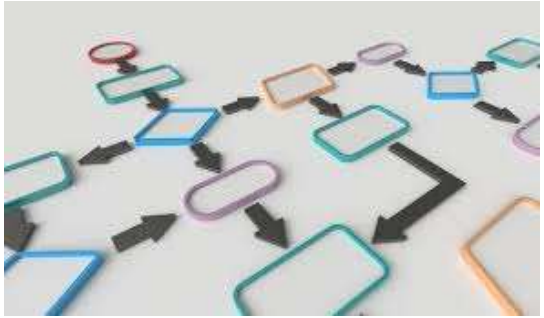
Benefits

- Provides a time-efficient means of assessing acquisition programs, development projects, initiatives, and capabilities
- Establishes confidence in the ability to achieve mission objectives
- Can be self-applied or expert led

Cybersecurity Engineering Review (CSER)

What

- Evaluates an acquisition program's security practices for conformance to accepted CSE practices



Why

- Understand the effectiveness of an acquisition program's cybersecurity practices
- Develop a plan for improving a program's cybersecurity practices

Benefits

- Establish confidence in a program's ability to acquire software-reliant systems across the lifecycle and supply chain
- Reduce cybersecurity risk of deployed software-reliant systems

Security Engineering Risk Analysis (SERA)

What

- A systematic approach for analyzing complex security risks in software-reliant systems and systems of systems across the lifecycle and supply chain

Why

- Build security into software-reliant systems by addressing design weaknesses as early as possible (e.g., requirements, architecture, design)
- Assemble a shared organizational view (business and technical) of cybersecurity risk

Benefits

- Correct design weaknesses before a system is deployed
- Reduce residual cybersecurity risk in deployed systems
- Ensure consistency with NIST Risk Management Framework (RMF)

Contact Information

Roman Danyliw

SEI Deputy Chief Technology Officer
Telephone: +1 412.268.5466
Email: rdd@cert.org

Chris Inacio

Chief Engineer
CERT Division
Telephone: +1 412.268.3098
Email: inacio@cert.org

Geoff Sanders

Senior Network Defense Analyst
Telephone: +1 703.247.1393
Email: gtsanders@cert.org

Tim Morrow

Technical Manager, Situational Awareness
Telephone: +1 412.268.4792
Email: tbm@cert.org