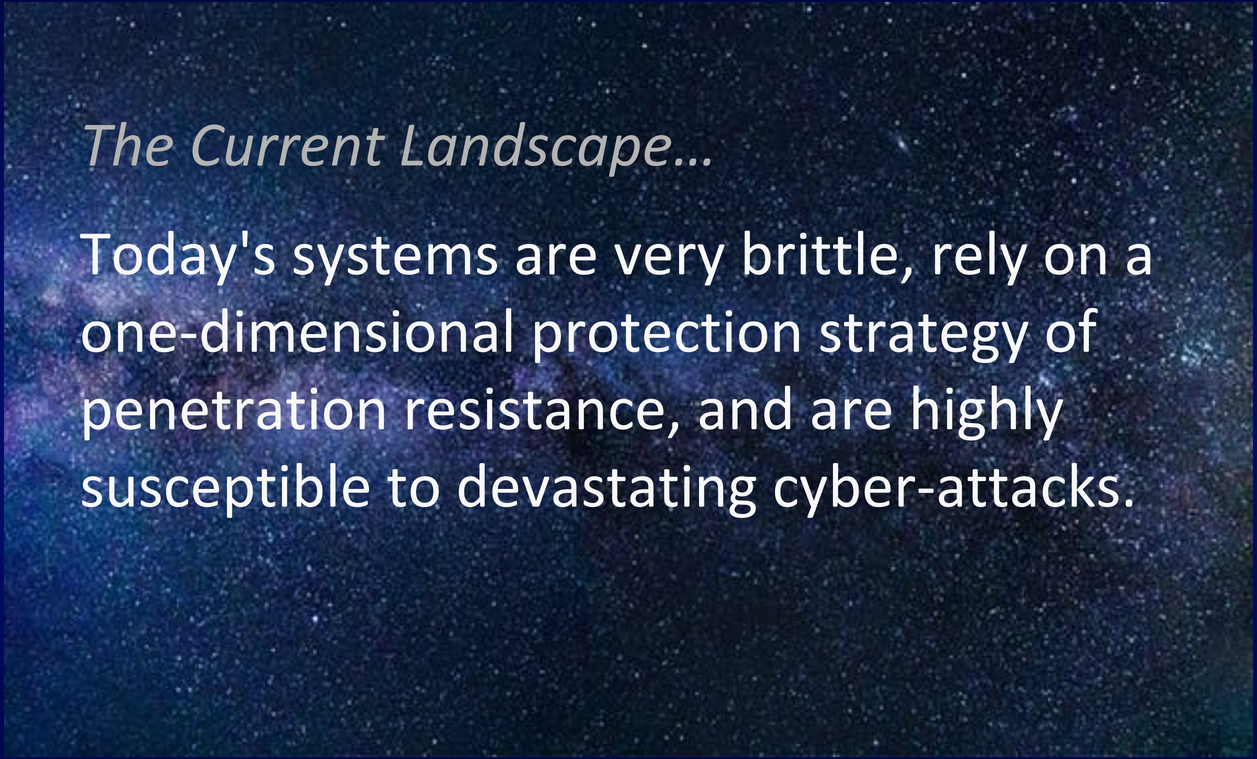
When Perimeter Defenses Are Compromised

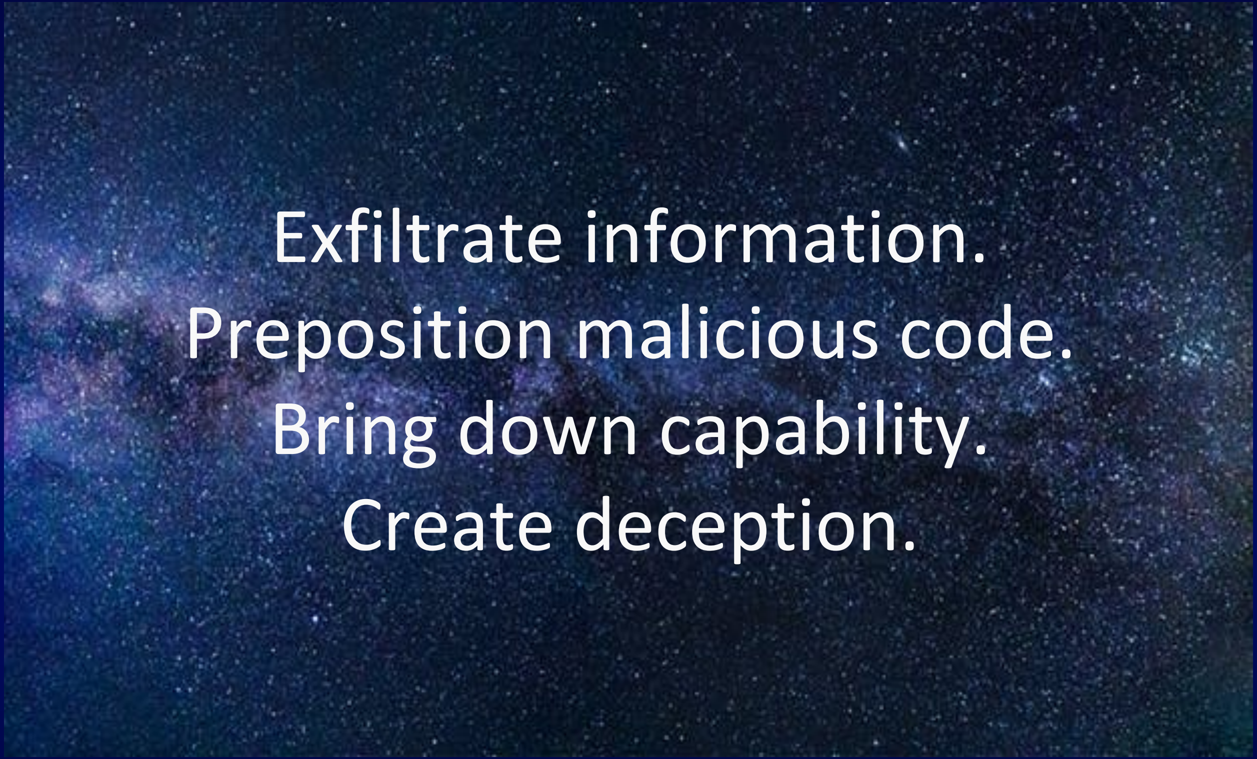
Applying Zero Trust Concepts to Achieve Cyber Defense-In-Depth



The Current Landscape…

Today's systems are very brittle, rely on a one-dimensional protection strategy of penetration resistance, and are highly susceptible to devastating cyber-attacks.

The adversaries are relentless.



Exfiltrate information.

Preposition malicious code.

Bring down capability.

Create deception.

- Resilient Military Systems and the Advanced Cyber Threat
- Cyber Supply Chain
- Cyber Deterrence

DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD
TASK FORCE REPORT:
Resilient Military Systems and the Advanced Cyber Threat
January 2013
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNO
WASHINGTON, D.C. 20301-3140

DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD
TASK FORCE ON
CYBER DETERRENCE
February, 2017
OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140

DSB Task Force on
CYBER SUPPLY CHAIN

Defense Science Board Reports

Defending cyberspace in 2020 and beyond.

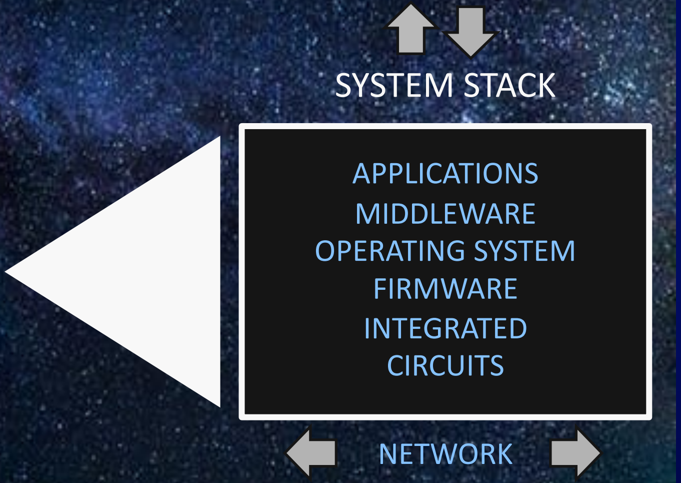
The Problem…

A one-dimensional protection strategy of penetration resistance and perimeter defense is inadequate – especially for critical systems and high value assets.

Another Problem…

Little or no understanding of what is in the ”black box.”

Transparency
Traceability
Visibility
Assurance



SYSTEM STACK

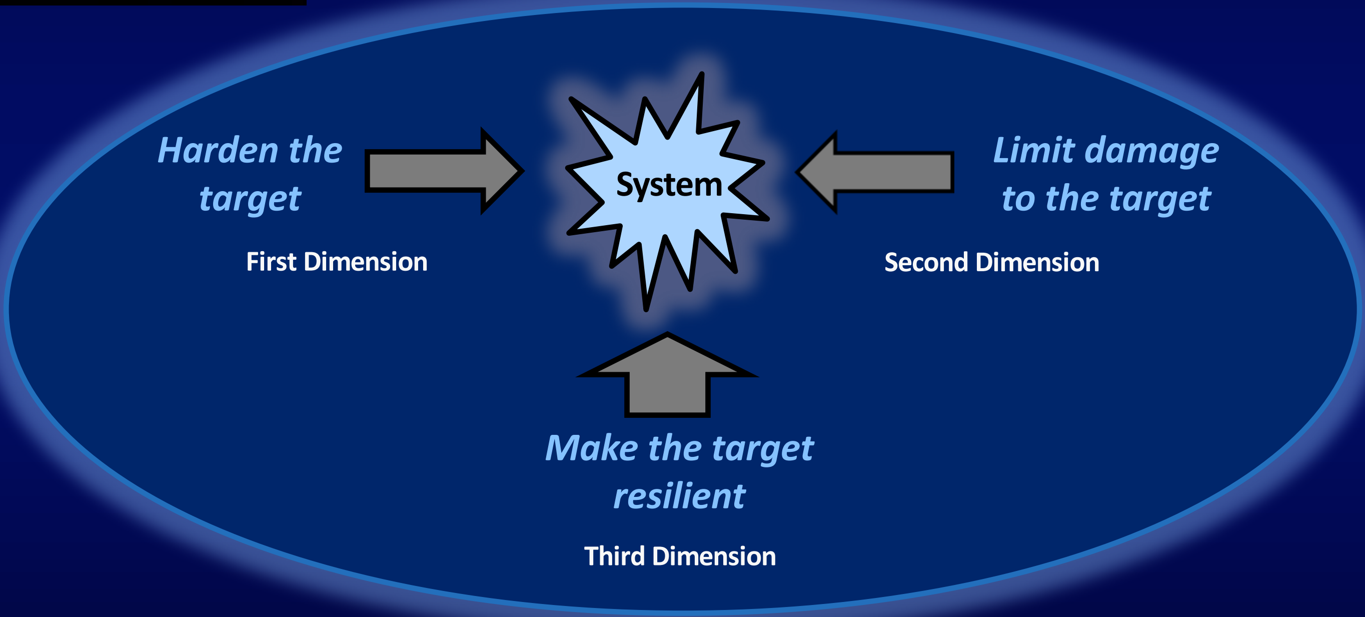
APPLICATIONS
MIDDLEWARE
OPERATING SYSTEM
FIRMWARE
INTEGRATED CIRCUITS

NETWORK

The Solution…

Adopt a multi-dimensional protection strategy that includes developing damage limiting system architectures and cyber resilient systems.

Reducing susceptibility to *cyber threats* requires a multidimensional strategy.



Harden the target

First Dimension

System

Limit damage to the target

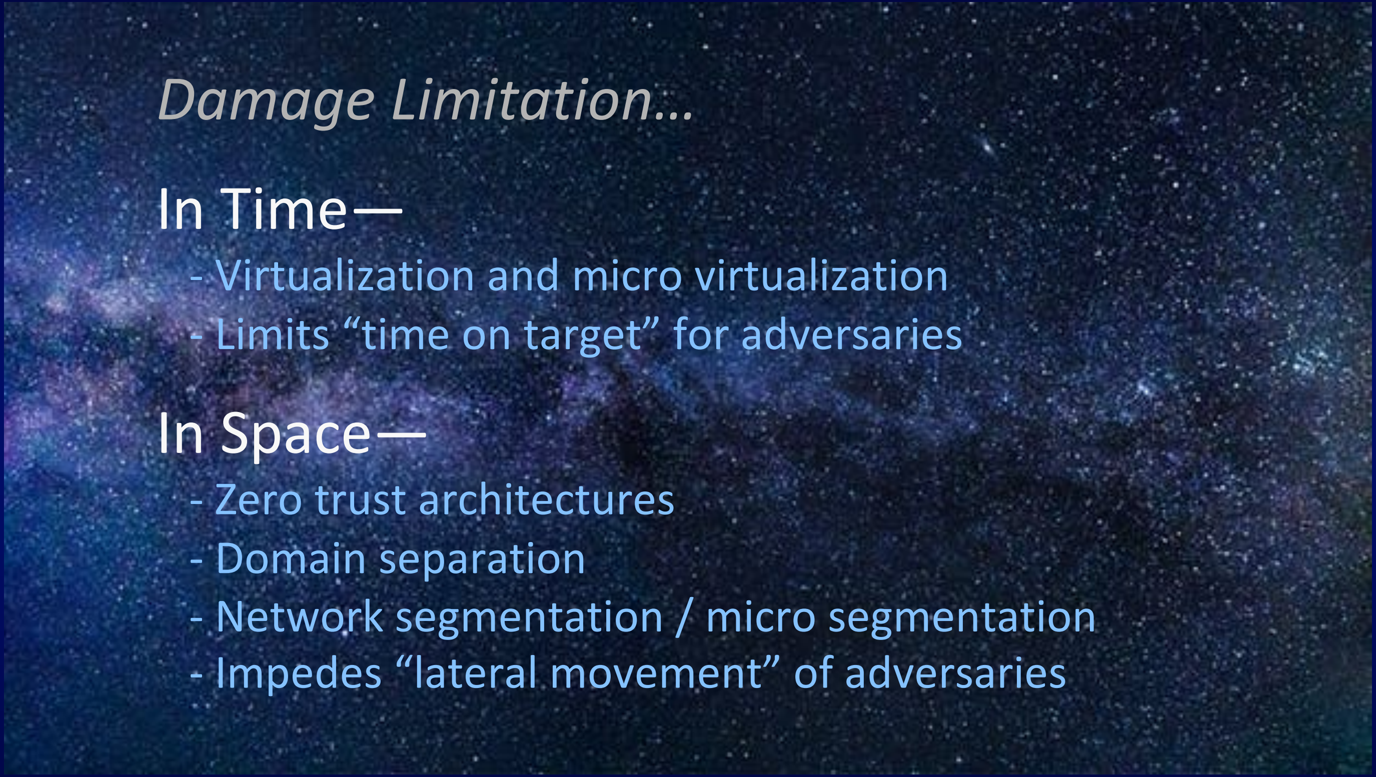
Second Dimension

Make the target resilient

Third Dimension

Cyber Resiliency

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.



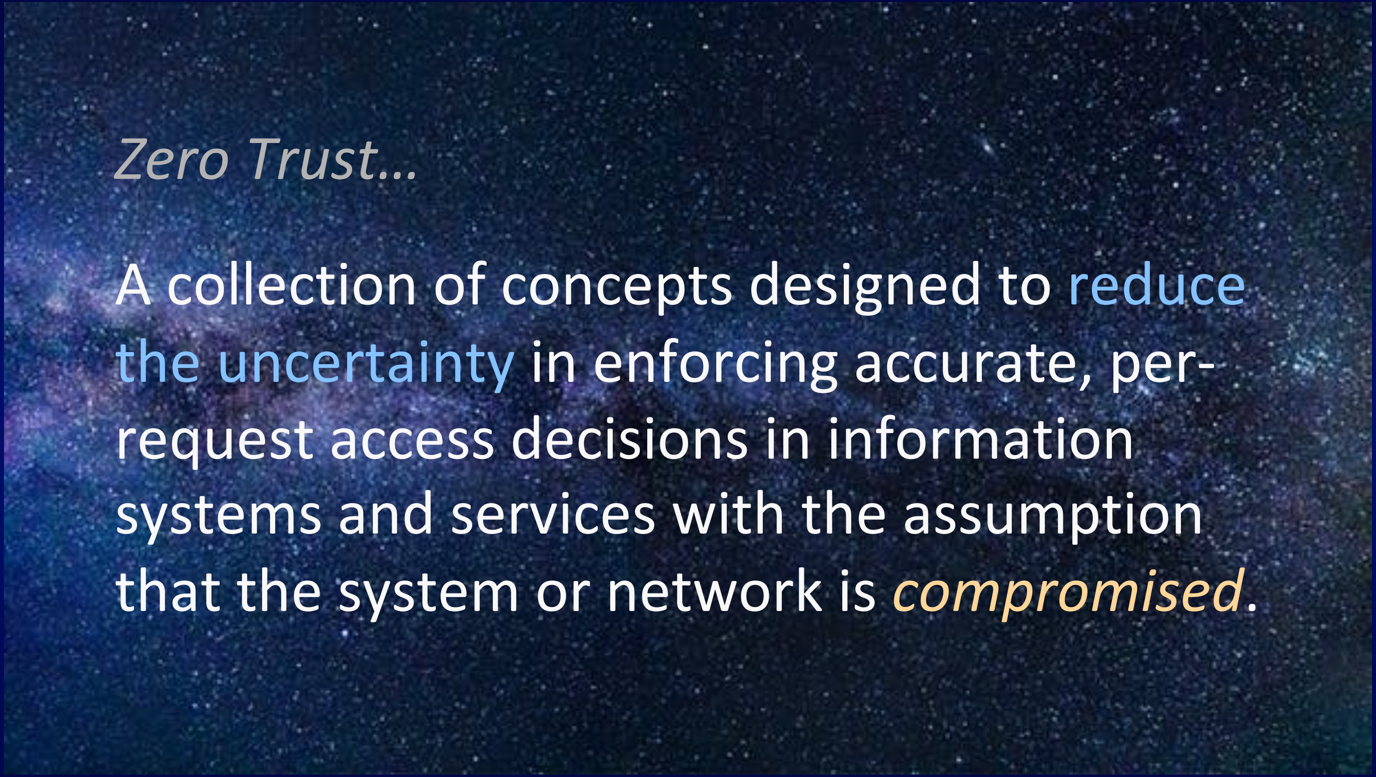
Damage Limitation…

In Time—

- Virtualization and micro virtualization
- Limits “time on target” for adversaries

In Space—

- Zero trust architectures
- Domain separation
- Network segmentation / micro segmentation
- Impedes “lateral movement” of adversaries



Zero Trust…

A collection of concepts designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services with the assumption that the system or network is *compromised*.

Zero Trust Architecture…

An enterprise’s security plan that employs zero trust concepts and includes component relationships, workflow planning, and access policies.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

DATA AND COMPUTING SERVICES ARE CONSIDERED RESOURCES

A network may be composed of many different classes of devices including devices with a small form factor that send data to aggregators or storage; software as a service (SaaS); systems sending instructions to actuators, and other functions.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ALL COMMUNICATIONS ARE SECURED REGARDLESS OF NETWORK LOCATION

Network location does not imply trust. Access requests from resources located on an enterprise-owned network (e.g., inside a traditional network perimeter) must meet the same security requirements as access requests from any other nonenterprise-owned network.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ACCESS TO INDIVIDUAL RESOURCES IS GRANTED ON A PER-SESSION BASIS

Trust in the requester is evaluated before the access is granted. This could mean only “sometime previously” for a particular transaction and may not occur directly before initiating a session or performing a transaction with a resource.

Authentication and authorization to one resource does not automatically grant access to a different resource.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ACCESS TO RESOURCES IS DETERMINED BY DYNAMIC POLICY

The dynamic policy includes the observable state of client identity, application, and the requesting asset, and may include other behavioral attributes.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

ENTERPRISE-OWNED AND ASSOCIATED DEVICES ARE IN THE MOST SECURE STATE POSSIBLE

The security of devices is driven by mission or business requirements.

Enterprises continuously monitor devices to ensure those devices maintain their security posture.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

RESOURCE AUTHENTICATION AND AUTHORIZATION ARE DYNAMIC AND STRICTLY ENFORCED – BEFORE ACCESS IS ALLOWED

Constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communications.

Identity, Credential, and Access Management (ICAM) and asset management systems are expected capabilities for an enterprise.

Zero Trust Concepts

SYSTEMS SECURITY ENGINEERING

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

THE SECURITY POSTURE OF THE ENTERPRISE IS CONTINUOUSLY IMPROVED BY MONITORING THE STATE OF THE NETWORK AND COMMUNICATIONS

An enterprise collects data about network traffic and access requests, which is then used to improve policy creation and enforcement.

Data can also be used to provide context for access requests.

Zero Trust Architecture in the System Life Cycle

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal

NIST SP 800-160 Volume 1

NIST Special Publication 800-207

Zero Trust Architecture

Second Public Draft

https://doi.org/10.6028/NIST.SP.800-207-draft2

NIST Special Publication 800-160, Volume 1

Systems Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

https://doi.org/10.6028/NIST.SP.800-160v1

NIST Special Publication 800-160, Volume 2

Developing Cyber Resilient Systems

A Systems Security Engineering Approach

https://doi.org/10.6028/NIST.SP.800-160v2

NIST SUPPORTING INITIATIVES

Zero Trust Architecture Project

https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

zta-nccoe@nist.gov

Systems Security Engineering Project

https://csrc.nist.gov/Projects/Systems-Security-Engineering-Project

sec-cert@nist.gov

100 Bureau Drive Mailstop 7770
Gaithersburg, MD USA 20899-7770

Email
ron.ross@nist.gov

LinkedIn
www.linkedin.com/in/ronrossecure

Web
csrc.nist.gov

Mobile
301.651.5083

Twitter
@ronrossecure

Comments
sec-cert@nist.gov