Design Code Basis for Secure Cyber Resilient Engineering

Foundation for a Secure System

Presented to NDIA Systems and Mission Engineering Conference
Orlando, Florida
November 2022

Melinda Reed
Director, Systems Security
Office of Under Secretary of Defense for Research and Engineering
Science and Technology Program Protection

Mark Winstead
Principal Chief Engineer, Systems Security
The MITRE Corporation

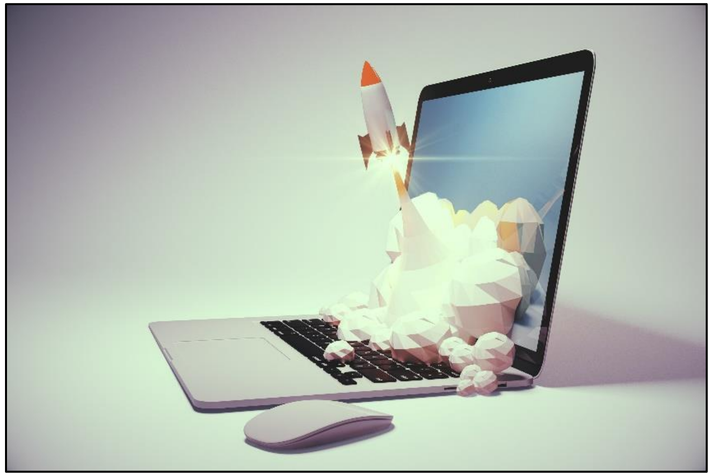
Agenda

- **The Need**
- **The Concept**
- **History – Trusted Computer Security Evaluation Criteria (TCSEC)**
- **Design Code Basis for Secure Cyber Resilient Engineering (SCRE)**
- **Production Nucleus**
- **What the Design Code Will Establish**

The Need for Design Code

- **Design code: *criteria* to guide activities to establish and mature the design of trustworthy, secure, and resilient weapon systems**

- **The criteria is targeted for use by system engineers, architects, designers, and developers for activities such as:**
  - System requirements derivation and decomposition
  - System architecture development
  - System design definition
  - System analysis
  - Requirements analysis



- **Design code will assist in developing and executing SCRE practice activities and tasks**

Distribution Statement A: Approved for public release. DOPSR case #23-S-0024 applies. Distribution is unlimited.

The “Code” Concept

- ***Code* is a form of expression to a specific audience.**
- **Code addresses:**
  - Capability, performance, and constraints.
  - Verification methods and overview acceptable solutions.
- **Code is structured and phrased specifically to facilitate its use within the scope of control or authority of its intended audience.**

- **Code continuously evolves to reflect need changes, technology evolution, practitioners’ experience growth, and research and development.**
- **Examples in other domains:**
  - Building Code: A set of rules specifying standards for constructed objects. Its main purpose is to protect public health, safety, and general welfare.
  - Electrical Code: A set of regulations for the design and installation of electrical wiring in a building. The intention of a code is to provide standards to ensure electrical wiring systems that are safe for people and property.

History of Design Code: Trusted Computer Security Evaluation Criteria

- **The Trusted Computer Security Evaluation Criteria (TCSEC) was the first instance of design code for trustworthy secure design.**
  - It served as the basis for the design, development, and evaluation of trusted operating systems.
  - The design code basis for the TCSEC was the seminal work that established the principles, concepts, objectives, and capabilities of an inherently secure system.
- **TCSEC motivated efforts to refine and extend aspects of design code criteria and its representation.**
- **However, none of these efforts established a principled design code suitable for use in the engineering of trustworthy secure systems.**

Design Code Basis for SCRE (Concept)

- **The capabilities, properties, and characteristics that are necessary and inherent to any trustworthy secure and resilient system**
- **Design code basis**
  - Enables the system to satisfy stakeholder expectations but is not dependent on any specific protection requirements
  - Encompasses
    - The core security protection mechanisms for the system to function security
    - The capability of the system to protect itself
  - Enables
    - The system to deliver the protection capability that fulfills the stakeholder’s protection needs

SCRE Design Code (Principled Basis)

- ***Design for Security and Cyber Resiliency* expectations (DoD Instruction 5000.83)**
  - Manage access to, and use of, the system and system resources
  - Be structured to protect and preserve system functions or resources
  - Maintain priority system functions under adverse conditions
  - Interfaces with the DoD Information Network or other external services
  - Monitor, detect, and respond to security anomalies
  - Be configurable to minimize exposure of vulnerabilities
- **Transforming these expectations led to further characterization of the *protection nucleus* for secure cyber resilient systems**

Protection Nucleus

- **The concept of protection capabilities and characteristics that are necessarily an inherent part of any secure system (Anderson Report*) expands to be the *protection nucleus***

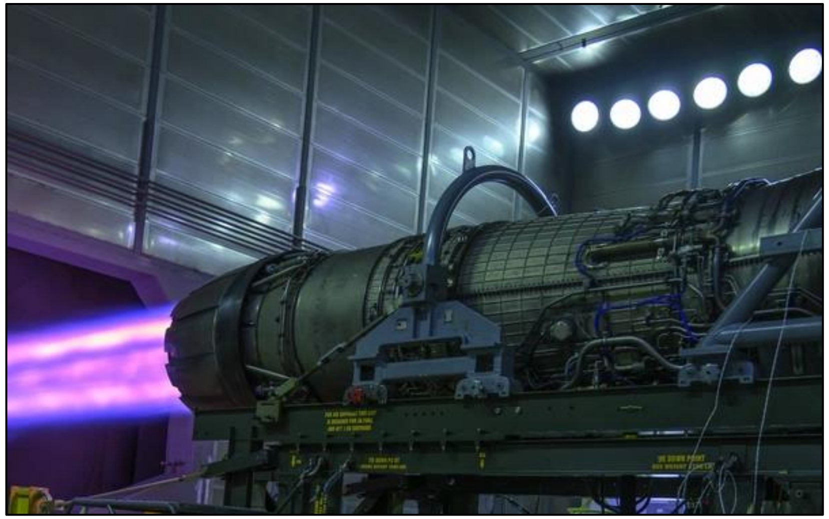
- **Key protection functions**
  - Protect what the system does functionally
  - Protect the interfaces necessary to provide functionality
  - Protect the configuration that determines the functionality
  - Protect the data associated with all the above

- **Core capabilities for the protection nucleus**
  - *Mediated Access*: enforce authorizations for all system interactions (internal and with external)
  - *System Control*: achieve only the intended system behaviors and outcomes associated with the authorization enforced by mediated access, and prevent and limit loss

*J. P. Anderson, "Computer Security Technology Planning Study, ESD-TR-73-51 Volume 1, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC)," 1972. AKA The Anderson Report

Design Code Criteria Development

- **Criteria for the *protection nucleus functions, capability, and its mechanisms***
- **Criteria for the *system***
  - To enable success of the nucleus
  - To not interfere with nucleus function
- **Criteria for *related engineering activities*, including verification**



Next Steps

- **Work with industry for inputs**

- **Continue activities to standardize SCRE practice to inform specific needs in design code**

- **Pull applicable criteria from existing documents and build additional candidate criteria for comment**

Questions?

References

- J. P. Anderson, "Computer Security Technology Planning Study, ESD-TR-73-51 Volume 1, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC)." 1972. AKA The Anderson Report.

- Department of Defense, “DoD Instruction 5000.83: Technology and Program Protection to Maintain Technological Advantage.” July 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500083p.pdf

- National Research Council, “Computers at Risk: Safe Computing in the Information Age.” 1991. https://doi.org/10.17226/1581