34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

A Principled Approach for Systems Engineers

Secure Design

Common practice in some communities is to select and overlay systems with security controls as a primary means to address security concerns. But as observed in a Rand Report, “Poor engineering is very difficult to mitigate by overlaying security controls …”

NIST SP 800-160 V1 R1

As a community, we've moved from plugging holes in operation or shortly before fielding (i.e., bolting on) to plugging holes in design phase (i.e., baking in) - and call that "secure by design".

But we still aren't avoiding holes during design - all our activity tends to be assessing holes and planning the plugs.

And where we need plugs, how do we support those plugs?

Work:

- OUSD(R&E) System Security
- Workshops for SysSec
- US National Institute of Standards & Technology (NIST)
- And Partners

Summary

Keys for Secure Design

- Understand the Desired Outcome
- Concepts
  - Think Strategically
  - Control
  - System Functionality
  - Assured System Trustworthiness
  - Inherently Secure Design
  - Adequately Secure

Derived multiple years work
Public released materials sample

- NIST
  - Engineering Trustworthy Secure Systems (nist.gov)
- OUSD(R&E) System Security Directorate
  - Concepts and Vocabulary
  - Interpreting “Cyber”
  - Security and Resilience Interpretation
  - Trustworthy Design Principles & Loss Control Design Principles
  - Strategic Considerations for Design
  - SCR Design Order of Precedence
  - Design Basis Adversity
  - Engineering the Protection Nucleus
  - System Trustworthiness and Assurance
  - Loss Control Objectives
  - Concept of Secure Function
  - Adequately Secure
  - Inherently Secure Design
  - Technical Protection Risks and Issues Part 1
  - System Design Guidance

Understanding the Desired Outcome

A **secure system** is one that meets the expectation that it does not exhibit behavior, produce outcomes, or lead to a state that:

- Violates rules that specify authorized and intended behaviors and outcomes,
- Causes an unacceptable loss of assets (i.e., anything of value to a stakeholder), or
- Constitutes an unacceptable asset loss.

Consequently:

The SE's responsibilty is that the design, once implemented,

- maximizes the certainty and
- minimizes the uncertainty

of achieving

- intended and only intended behaviors and outcomes for intended users, despite adversity (i.e., negative influences on the system).

Functionally Interpreting Security (Insight June 2022 article w/McEvilley)

Concepts for Secure Design: systems engineering role

Think Strategically	• strategic approaches necessary for engineering systems for contested environments
System Protection Control	• a secure design accounts for the need to provide system control to protect the system and assets that are potentially impacted by system failures and misuse
System Functionality	• All system functionality can impact security!
Assured System Trustworthiness	• Functionality without assurance increases risk
Inherently Secure Design	• How to engineer using design order of precedence
Adequately Secure	• Security is an ideal, what suffices?

Think Strategically

- Security should be approached strategically to frame the use of tactics.
- Security should not be treated as a risk management problem
  - It is not “add controls from a catalog”
- Young & Leveson observed the better approach is to think of assuring the delivery of desired capability with desirable behaviors
  - think in terms of strategically maximizing success instead of minimizing failure with tactics

Strategic elements/considerations

- Principled Basis (e.g., mediated access, least privilege)
- Optimized Protection Basis – inherently secure design
- Effect-based and cause-informed
  - Focus on effects of loss
- Broad effectiveness against adversity
  - Negative influences are all around
- Assured trustworthiness
  - Is it trusted to be secure?
- Usability
  - Users are partners in security
- Evolvability
  - Things change

N. Leveson, W. Young *An Integrated Approach to Safety and Security Based on Systems Theory*, Communications of the ACM, Vol 57 No. 2 Feb 2014

System Protection Control

- Security is about control (not “controls”)
- Effect-oriented and fulfills its responsibility by
  - Avoiding preventable losses,
  - When loss cannot be avoided, limiting to tolerable levels, when possible, and
  - Avoiding additional loss beyond what has occurred.

System Protection Control

- System Protection Control has passive and active aspects
  - Passive: structure & architecture
    - provide the infrastructure to group, separate, and partition elements
    - to establish the interfaces and interconnections between system elements;
    - to enable control and data flow between system elements.
    - Do not exhibit behavior.
    - Determines how the system is composed to exhibit/product the authorized and intended system behaviors and outcomes
  - Active: devices & mechanisms
    - Exhibit their own behavior and produce outcomes.
    - Initiate data and control flows and deliver system-level capability through composed emergent behavior and side-effects.
    - Enabled and constrained by the passive aspects
    - Includes active constraints

System Protection Control

- Core responsibilities
  - Mediates the Accesses
  - Controls the anomalous behaviors and outcomes including avoid/prevent
- The control ideally is non-bypassable, evaluatable, always-invoked, and tamper-proof

System Functionality: Two parts

- Intended System Functionality
  - Is the desired functionality fully described?
  - Can the implemented Intended System Functionality cause loss?
- Security Functionality
  - the set of mechanisms that deliver the capability to enforce constraints on the system behaviors and outcomes, and the mechanisms and the passive architecture features that support
  - Is the security functionality protected?

Assured System Trustworthiness

- The design must support assured system trustworthiness
- Assured system trustworthiness is a principled, well-reasoned, and objective evidence-supported decision basis for the extent of trust given to aspects of system functionality
- Deficiencies with assurance means uncertainty exists, and risk is the effect of uncertainty on objectives
  - assurance controls risk.

Three criterion types describe the decision basis for trustworthiness:

- Criteria for describing the trustworthiness claim.
- Criteria for reasoning to demonstrate the claim is achieved or not achieved.
- Criteria for objective evidence used to support the reasoning.

Assured System Trustworthiness

- The design must support assured system trustworthiness
- Assured system trustworthiness is a principled, well-reasoned, and objective evidence-supported decision basis for the extent of trust given to aspects of system functionality
- Deficiencies with assurance means uncertainty exists, and risk is the effect of uncertainty on objectives
  - assurance controls risk.

Assured System Trustworthiness

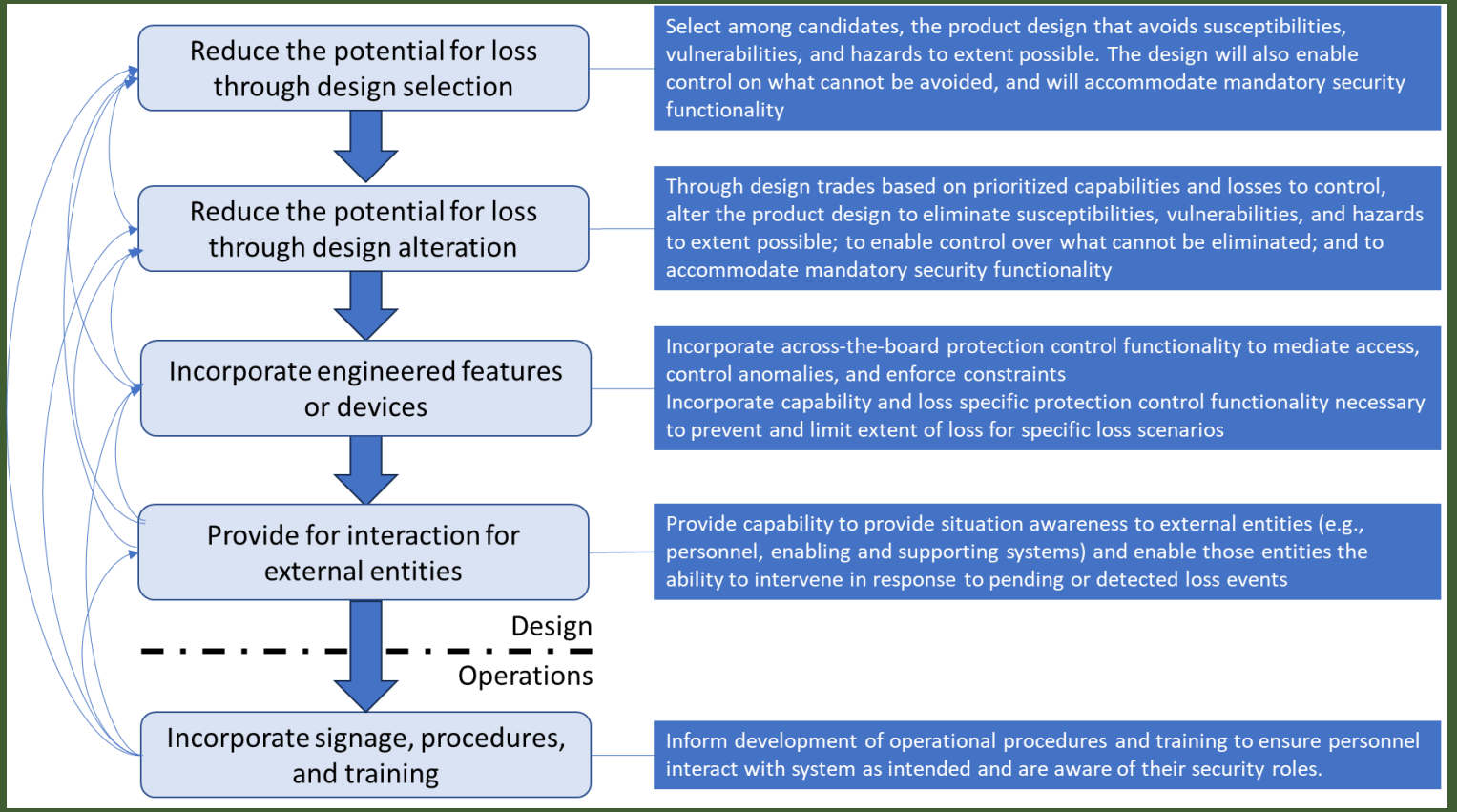
- Rigor with systems engineering needed to provide quality evidence
  - **What activities are conducted**
    - The activities' planning and their control conducted to establish and mature an assured trustworthy design.
  - **How activities are conducted**
    - The selection and use of the personnel, methods, materials, processes, approaches, and tools, and techniques necessary to conduct the planned activities.
  - **The results as conducted**
    - The adequacy, sufficiency, completeness, comprehensiveness, and effectiveness of the activities' results.

Inherently Secure Design

A hazard (conditions leading to loss), susceptibility (“inability to avoid a hit”), and/or vulnerability (“inability to take a hit”) may lead to loss

The intent with inherently secure design is fewer innate hazards, susceptibilities, and vulnerabilities than would exist otherwise

Fewer hazards, susceptibilities, and vulnerabilities address epistemic uncertainty (uncertainty due to lack of knowledge).



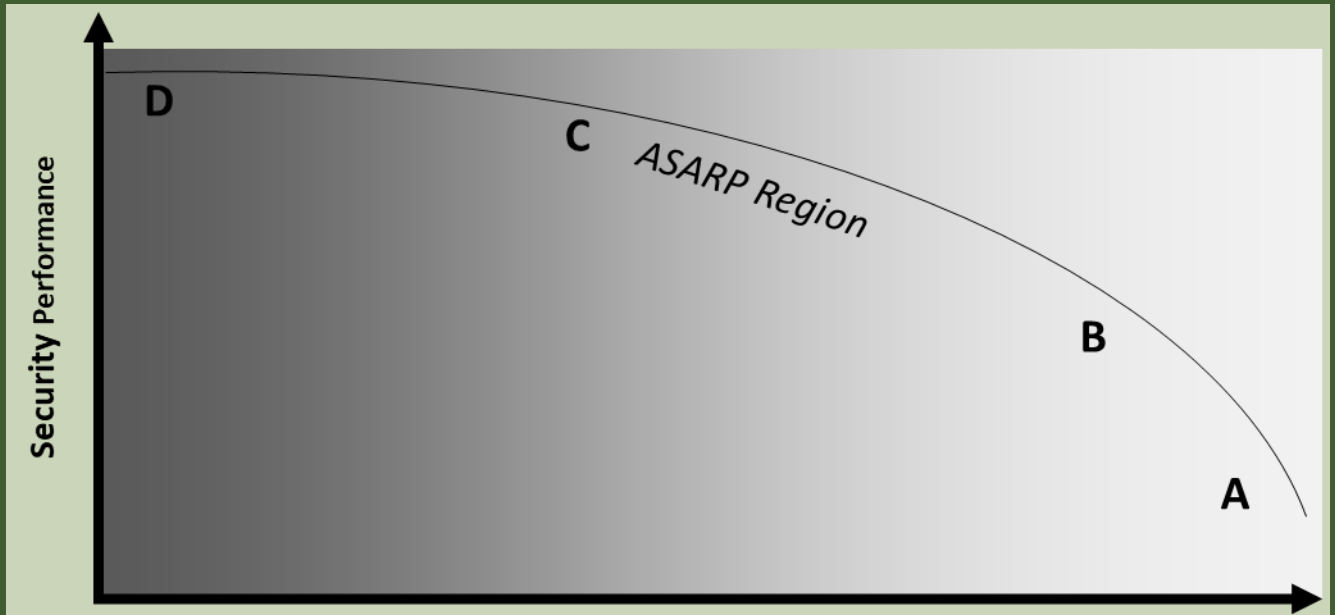
The Design Order of Precedence is a means to engineer for inherently secure design

Adequately Secure

Security is not for security's sake, rather enables the system.

The concept of adequately secure enables meaningful evidence-based judgments about the idealistic nature or interpretations of security definitions and informs proper trades.

The basis for claims about adequate security has roots in the definition of system security cited. Consequently, the claims for adequately secure address whether the system is as secure as reasonably practicable (ASARP) within reasonable impacts on cost, schedule, and technical performance.



(A) Large increases in system security can be achieved with little cost, schedule, or capability impact
(B) Basic security issues addressed but significant opportunity to improve security while meeting other system objectives
(C) The ASARP is reached but increases in security possible without exceeding tolerances on other system objectives
(D) No further achievable security possible

Closing

- Through numerous efforts for sponsors and with other organizations, our team at MITRE has been partnering to advance systems engineering for contested operational environments in manners aligned with INCOSE Systems Engineering Vision 2035
- The paper summarizes much of the continuing work specifically on secure design, connecting concepts across various products.
- The hope is others will build upon it and join in the informal partnerships of the larger community to further advance systems engineering for security.

Questions/Discussion

mwinstead@mitre.org

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS