Acquisition Research Program:
Creating Synergy for Informed Change

Acquisition System Design Analysis for Improved Cyber Security Performance

Brad R. Naegle

Cyber Warfare: Asynchronous Strategy and Tactics

Types

- Passive
- Active
- Denial of Service
- Spoofing
- Artificial Intelligence

Sources

- Traditional Adversaries
- State Actors
- Non-State Actors
- Domestic Adversaries
- Small Teams & Individuals

Cyber Warfare Implications

- Extraordinary concern due to accelerating incidents, asynchronous nature, effectiveness against US systems, and perceived vulnerability
- US systems dependent on elements known to be potential cyber vulnerabilities: Software, anything that communicates, sensors, and networks
- Developing systems need to minimize and mitigate potential cyber vulnerabilities

The Problem

- The Defense Acquisition System cedes significant design control to the contractor and the PM needs visibility and control over design elements with potential cyber vulnerabilities

The Symptoms

- Successful cyber attacks on US systems and assets
- Fielded systems have unknown cyber vulnerabilities
- Reactive, system-level cyber vulnerability testing
- Costly and frustrating Risk Management Framework evaluation and compliance

The Underlying Causes

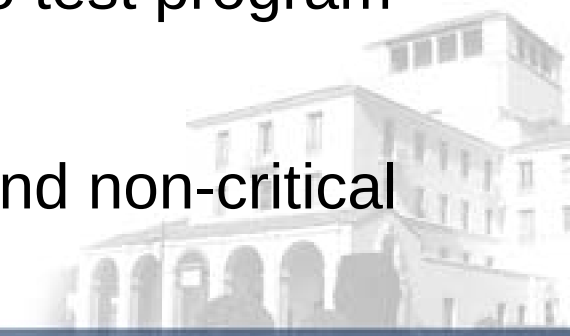
- The Defense Acquisition System
  - Driven by Capabilities-Based (JCIDS) and Performance-Based requirements (Performance Spec), that are designed to allow the contractor to control the design
  - ***Purposely vague to garner maximum innovation***
  - ***Likely to omit or poorly define cyber performance needed by the warfighter***
  - ***Provides only a glimpse at the operational environment through the Operational Mode Summary/Mission Profile***
  - Cyber Security needs typically not apparent to system designers

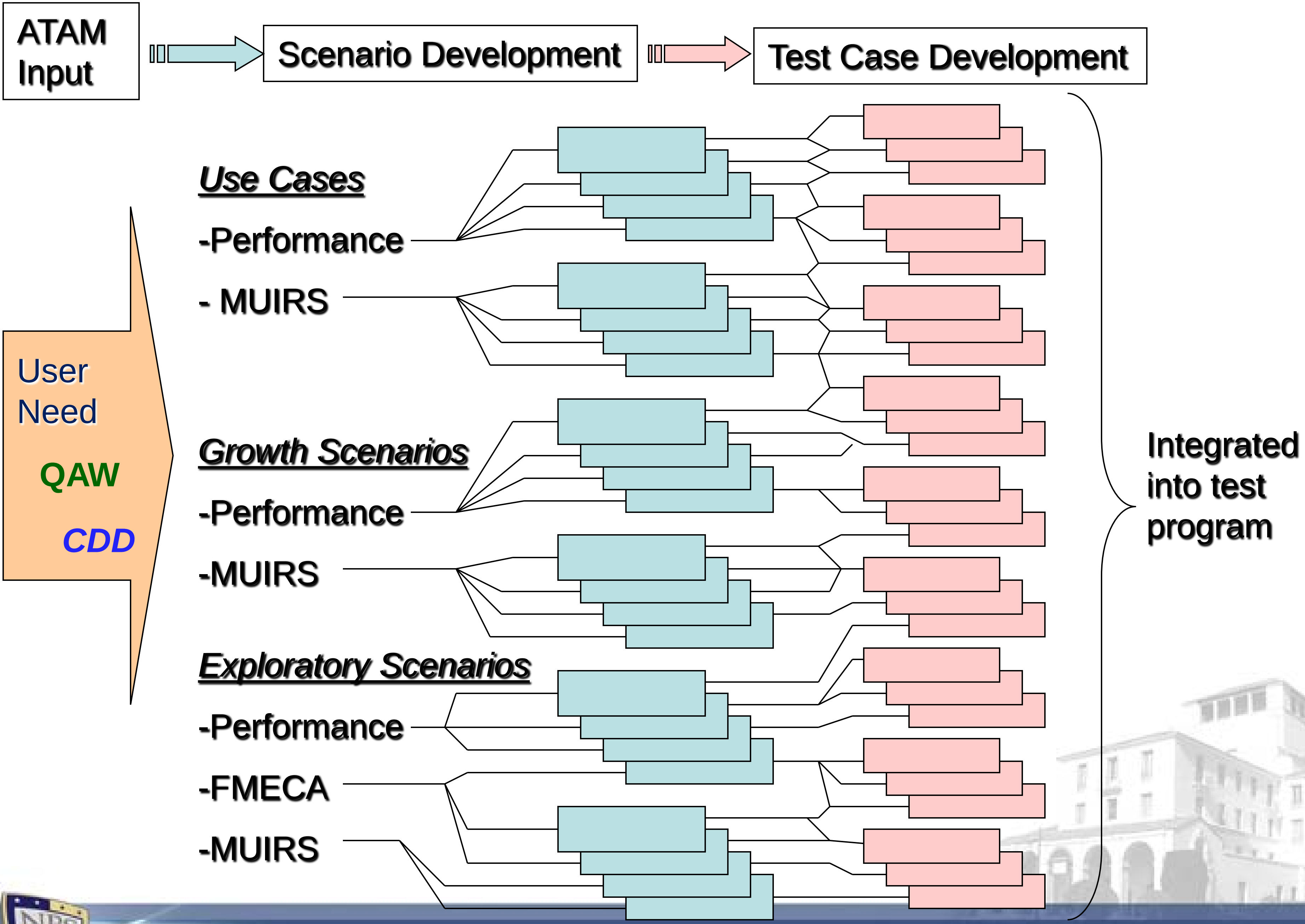
Cyber Vulnerabilities Control

- The PM must know and control potential cyber vulnerabilities on their systems
  - Thorough requirements and operational environment analyses to ensure cyber performance & potential vulnerabilities are ***known***
  - Design ***control*** over these elements and designation of potential vulnerabilities as Configuration Items (CI)
  - Control use of COTS components, especially software, in cyber vulnerable subsystems to avoid proprietary and data rights restrictions
  - Establish cyber test protocols for known system vulnerabilities to rapidly respond to new threats

Helpful Tools, Techniques, & Analyses

- SEI’s Quality Attribute Workshop (QAW)
  - A more complete inventory of cyber performance requirements
- MUIRS Analysis
  - Analyses of typical cyber vulnerable areas
- SEI’s Architectural Trade-off Analysis Methodology sm
  - Clarifies context and drives architectural design
  - Connects user needs to system design to test program
- FMECA
  - Identifies cyber vulnerabilities in critical and non-critical systems





ATAM Input

Scenario Development

Test Case Development

User Need

QAW

CDD

Use Cases

-Performance

- MUIRS

Growth Scenarios

-Performance

-MUIRS

Exploratory Scenarios

-Performance

-FMECA

-MUIRS

Integrated into test program

Summary

- PMs must ***know*** and ***control*** cyber vulnerabilities on their systems, which the DAS does not automatically support
- Using the tools, techniques, and analyses, will help identify and control vulnerabilities and establish testing protocols for new threats
- After gaining the full inventory of system cyber vulnerabilities, the RMF can be more efficiently and effectively supported