

Status Update

Security Profile Specification (SPS)

Michael McEvilly

21 August 2002



Overview

- Foundational points
- Specification Development
- The SPS
 - Where we were
 - Where we are
 - Where we are going
- Open Discussion

“The immediate [security] problems of cyber systems can be patched by implementing “best practices”, but not the *fundamental* problems.”

“In 1993, the Naval Research Laboratory did an analysis of some 50 security flaws and found that nearly half of them (22) were *part of the requirements specifications.*”

Wm. A Wulf, Ph.D.

President, National Academy of Engineering

AT&T Professor of Engineering and Applied Sciences, University of Virginia

before the

House Science Committee

U.S. House of Representatives

October 10, 2001



Set standards for homeland security technology

In order to encourage investment in homeland security science and technology efforts, the Department of Homeland Security, along with other federal agencies, would work with state and local governments and the private sector to build a mechanism for analyzing, validating, and setting standards for homeland security equipment. The Department would develop comprehensive protocols for certification of compliance with these standards. This activity will allow state and local officials to make informed procurement decisions.

National Strategy for Homeland Security

Office of Homeland Security

July 2002



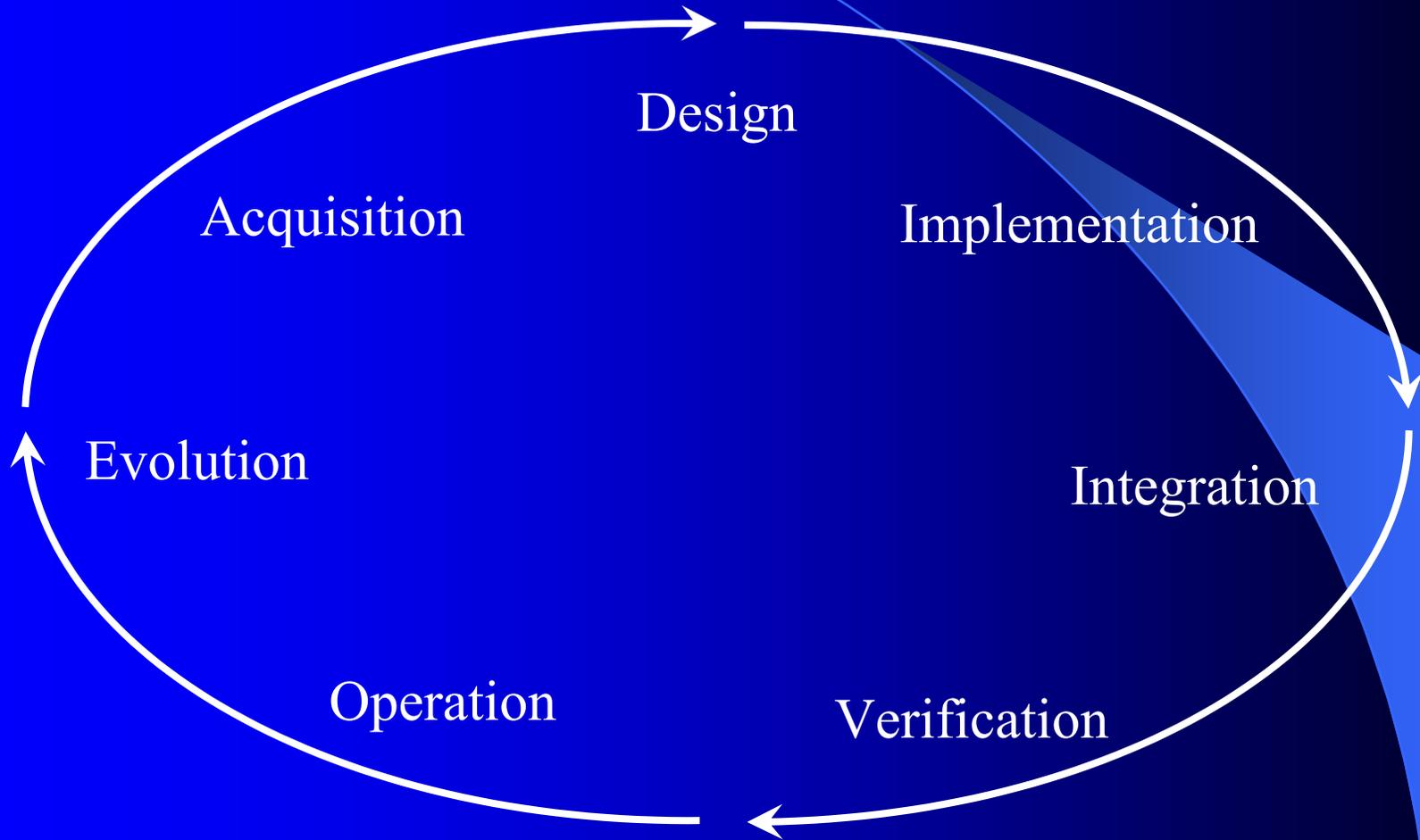
Specification Development

- Application of requirements engineering principles to establish
 - Necessary and sufficient **security**
 - Cost-effective **security**
 - Achievable **security**

... throughout the entire **system life-cycle**

The System Life Cycle

A Process of Processes



Obtaining Security

- Question: How do I get security?
 - Answer: It must be engineered in.
- Question: How do I know when its there?
 - Answer: Through assurance measures.
- Question: How do I obtain assurance?
 - Answer: It must be part of the engineering.

Establishing the Basis for Engineered Security

- The Security Case
 - Statement of security problem
 - Solution to security problem
 - Substantiating the effectiveness of the solution
- The security case parallels the “safety-case” concept used in development of safety-critical applications
 - Well proven in Aerospace (basis for FAA certification)

Requirements Specification Framework

“i.e., Protection Profile”

- Security component description
 - Security component application domain
 - Secure usage assumptions
 - Organizational security policies
 - Threats
 - Security Objectives
 - Security Requirements
 - Functional, Assurance
 - Rationale
- Statement of problem
- Statement of solution
- Substantiation of solution

Requirements Engineering

As a Component of Systems Engineering

- Focuses on establishing criteria and verifying compliance against criteria
 - Satisfactory to ALL stakeholders
 - For application to serve ALL stakeholders
- Security properties and verification activities
 - Must be engineered into the system
 - Must be consistent with imposed constraints
 - Functional
 - Performance
 - Safety

Security Engineering Process

- ✓ *verify* ● Vulnerability/Threat/Risk assessment
 - Determine priorities
- ✓ *verify* ● Develop policy
- ✓ *verify* ● Determine strategy to institute enforcement and countermeasure mechanisms
- ✓ *verify* ● Develop requirements
- ✓ *verify* ● Build
- ✓ *verify* ● Test
- ✓ *verify* ● Operate

The SPS

- An intermediate step in development of a PP
- A validated SPS will be translated into a CC compliant PP

SPS Development Difficulties

- Primary
 - No security policy basis
 - No security requirements basis
 - No vulnerability/risk basis
 - No acceptance test basis
- Secondary
 - Diverse industry domains
 - Little similarity across/within domains

Initial SPS Development Strategy

- Work through and within PCSRF to *identify*
 - Control system configurations
 - Control system vulnerabilities
 - Control system requirements

Course-Corrected SPS Development Strategy

- Work within industry domains to *collect information*
 - Control system configurations
 - Control system vulnerabilities
 - Control system requirements
- Work within PCSRF to *synthesize and document*
 - Control system configurations
 - Control system vulnerabilities
 - Control system requirements

New Strategy Trial

- Discrete Parts Manufacturing Vulnerability Workshop
 - Sponsored by National Center for Manufacturing Sciences (NCMS)
- Collected ~ 6 pages of notes
 - Security “Hot” Buttons
 - Asset Definition and Categorization/Weighting
 - Vulnerability Scenario

Analysis Findings

- So far – very good!
- Still not done
 - 1.5 pages of workshop notes generated 7 pages of refined information
 - ... and that is just the beginning
 - Many questions still to answer
 - Many issues raised
 - More questions to ask

Example

- Security “Hot” Button
 - Need to “SLAM” proof systems
- What is “SLAM”?
 - Application/use of push technology
- What is meant by “SLAM” proof
 - Restrict the capability to update configuration
- What is the real requirement???
 - Need for policy that is enforced

Assessment of NCMS Workshop

- a Success!
 - Extremely valuable information
 - ... after it is reviewed and structured
- Hot Buttons
 - 23 documented “buttons” during workshop
 - Analysis resulted in 9 categorical groupings

The Refined Nine

- Control System Access Control
- Communications Integrity
- Control System Integrity
- Intrusion Detection & Response
- Operational Assurance Maintenance
- Evolutionary Assurance Maintenance
- Operating Policy Analysis, Definition, Enforcement
- Collaborative Working Relationships
- Security Ownership

The Refined Nine

- **Control System Access Control**
- **Communications Integrity**
- **Control System Integrity**
- **Intrusion Detection & Response**
- **Operational Assurance Maintenance**
- **Evolutionary Assurance Maintenance**
- Operating Policy Analysis, Definition, Enforcement
- Collaborative Working Relationships
- Security Ownership

Where is the SPS Today?

- Document updated
 - Recommended changes
 - Results of discussion
 - New perspective
- Document enhanced
 - Captures findings from first pass of NCMS vulnerability workshop analysis

Where are we going?

- Obtain review and comment
 - Need greater response from PCSRF participants or their designated representatives
- Continue to flesh out document
- Target next industry and continue collecting information

Questions?

**Thank you
for your attention.**

Michael McEvilly

703.414.5002 (voice)

703.414.5066 (fax)

mam@decisive-analytics.com

www.commoncriteria.com

