A Systematic Approach to Information Systems Security Education

Joseph J. Simpson
Dr. Barbara Endicott-Popovsky

June 7, 2010

Overview

Introduction

Comprehensive Model of Information Systems Security (McCumber Cube)

Asset Protection Model (APM)

- Cognitive Complexity - Miller Index

Asset Cube

- System – Systems Engineering Community
- Target – Information Assurance Community
- Threat – Justice, Legal and IC Communities

Information Systems Security Framework

- System Framework
- Target Framework
- Threat Framework

Dynamic System Security Model

Preliminary Results from Team Use

Summary, Conclusions

Introduction

Purpose

- Establish an expanded conceptual model for asset protection

Constraints

- Human short-term reasoning capability
- Rate of technology and organizational change
- Involvement of multiple professional communities
- Expert knowledge differentiated from novice knowledge
- Lack of commonly accepted legal infrastructure

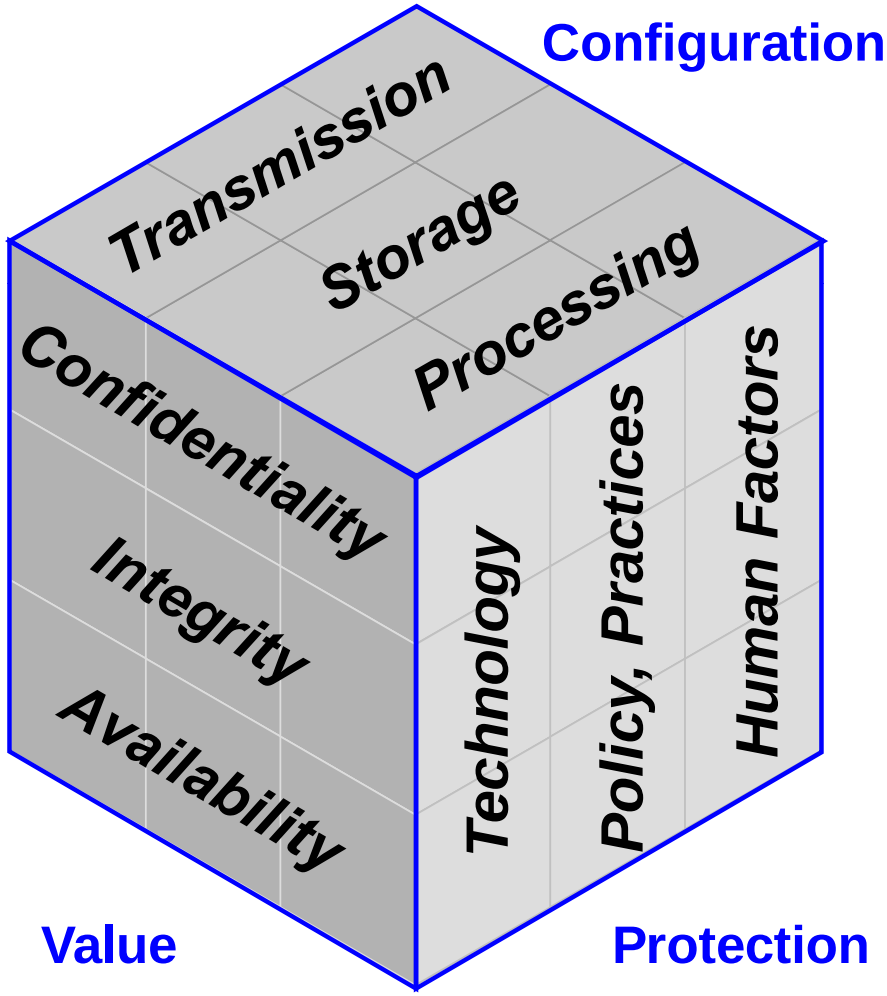
Proposed New Model

- Supports human reasoning capabilities
- Establishes recursively defined levels of abstraction
- Supports computer-enhanced reasoning at detailed level
- Implemented independent of organization and technology

Outcomes

- Conducted team test with CISO focus (one academic quarter)
- Strong positive feedback from team and instructor

McCumber Cube

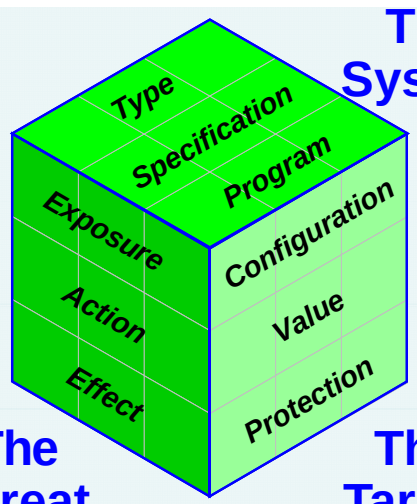


- Represents durable risk assessment model for information assurance (IA) community
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

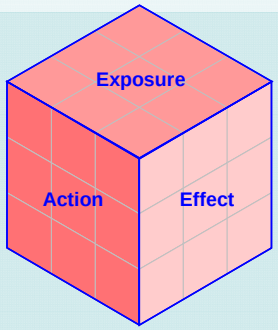
Asset Protection Model

Recursive design for adaptable computer support

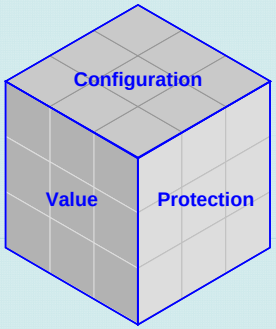
Highest Level of Abstraction – Level 1



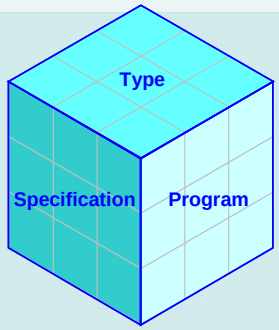
Abstraction Level 2



The Threat Cube

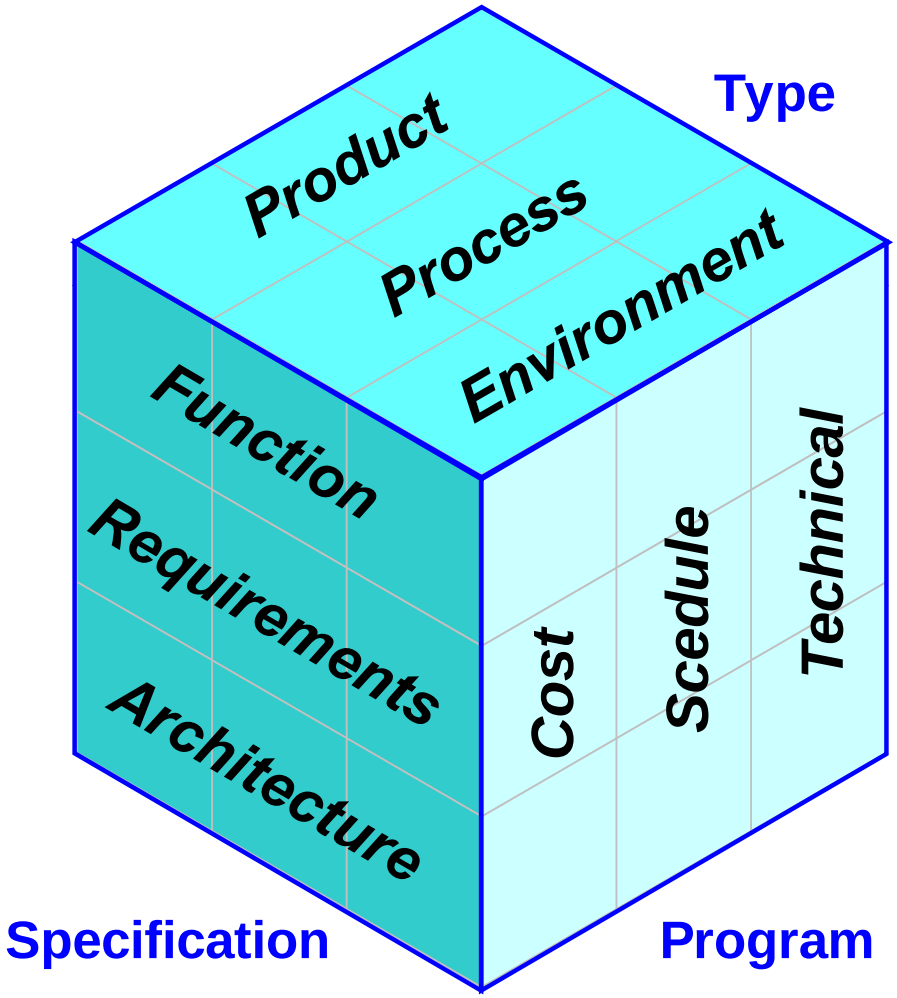


The Target Cube
[Domain-Specific]



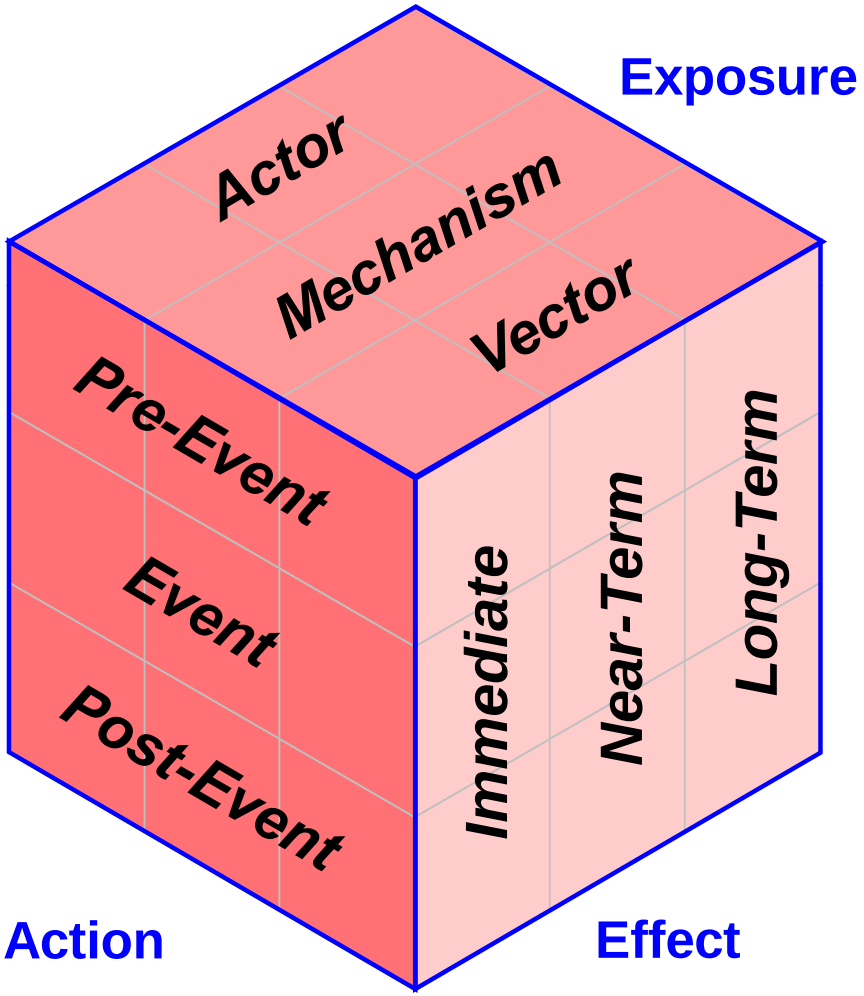
The System Cube

Asset Cube - System



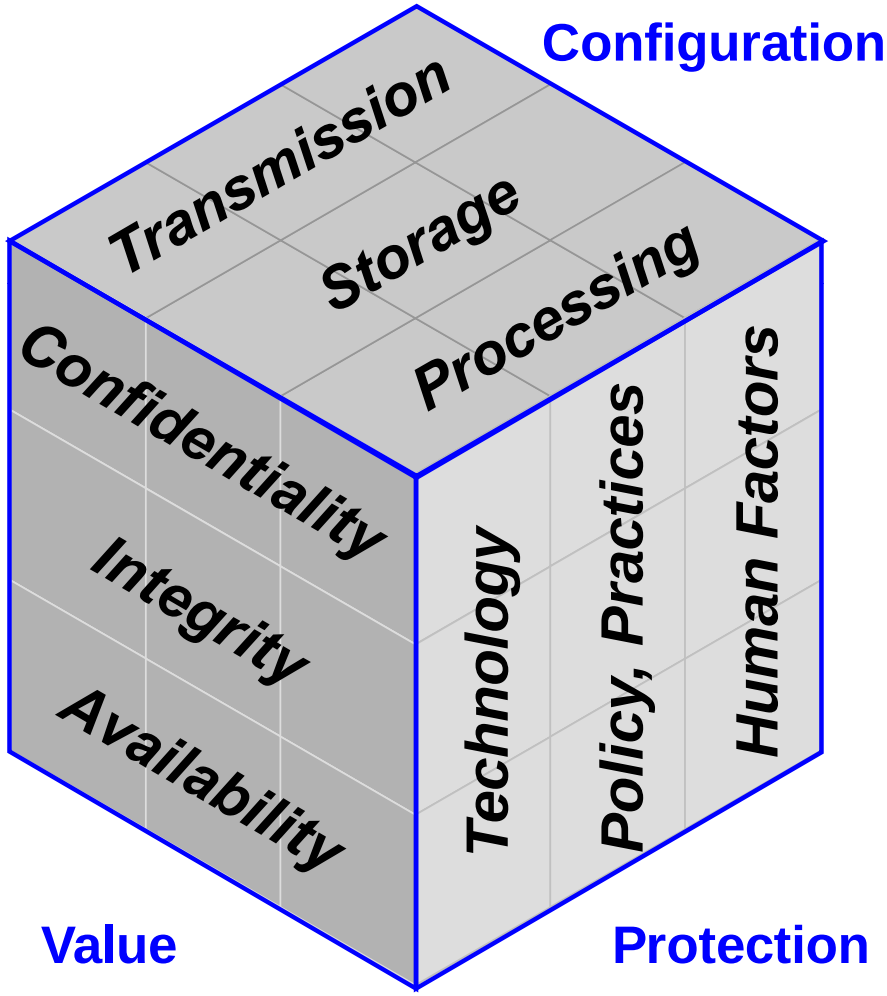
- Represents durable systems model for systems engineering (SE) community
- Configures to a ‘matrix’ of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

Asset Cube - Threat



- Represents durable threat model for Justice, Legal, and IC communities
- Provides level of detail to support information classification
- Configures to a ‘matrix’ of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

Asset Cube - Target



- Represents durable risk assessment model for information assurance (IA) community
- Configures to a 'matrix' of 9 elements
- Accommodates short-term human cognition capabilities
- Reflects structural design principles from systems science

APM Framework – 'Sub-Cube' Structure (1 of 3)

X Axis	Y Axis	Z Axis
System Type	Threat Exposure	Target Configuration
System Type	Threat Exposure	Target Value
System Type	Threat Exposure	Target Protection
System Type	Threat Action	Target Configuration
System Type	Threat Action	Target Value
System Type	Threat Action	Target Protection
System Type	Threat Effect	Target Configuration
System Type	Threat Effect	Target Value
System Type	Threat Effect	Target Protection

APM Framework – 'Sub-Cube' Structure (2 of 3)

X Axis	Y Axis	Z Axis
System Specification	Threat Exposure	Target Configuration
System Specification	Threat Exposure	Target Value
System Specification	Threat Exposure	Target Protection
System Specification	Threat Action	Target Configuration
System Specification	Threat Action	Target Value
System Specification	Threat Action	Target Protection
System Specification	Threat Effect	Target Configuration
System Specification	Threat Effect	Target Value
System Specification	Threat Effect	Target Protection

APM Framework – 'Sub-Cube' Structure (3 of 3)

X Axis	Y Axis	Z Axis
System Program	Threat Exposure	Target Configuration
System Program	Threat Exposure	Target Value
System Program	Threat Exposure	Target Protection
System Program	Threat Action	Target Configuration
System Program	Threat Action	Target Value
System Program	Threat Action	Target Protection
System Program	Threat Effect	Target Configuration
System Program	Threat Effect	Target Value
System Program	Threat Effect	Target Protection

APM Level 1 Interfaces

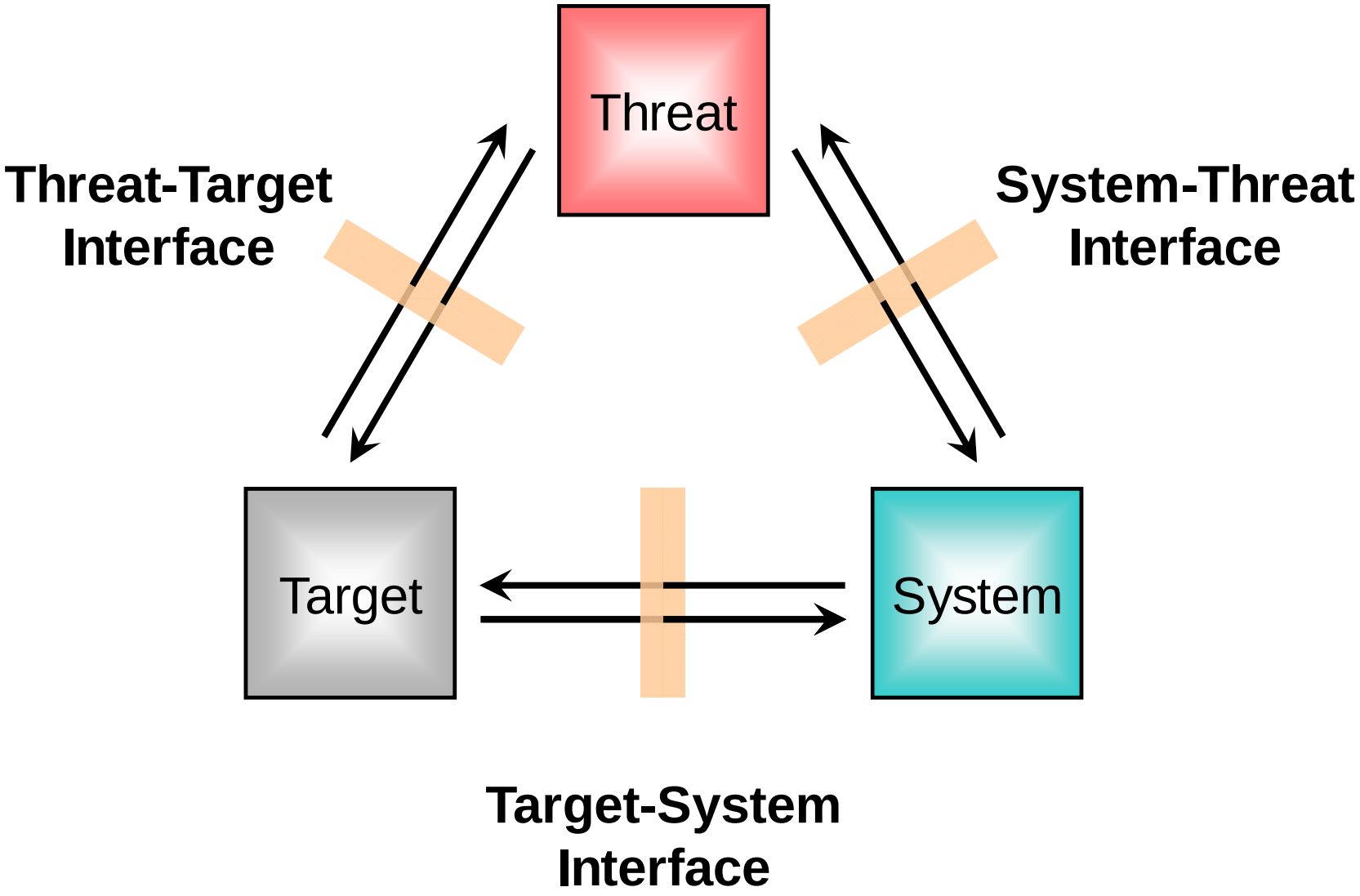
Interface Communications

- Well-defined interfaces with clear, structured patterns
- Experts can focus on their particular area of expertise
- Novices have a way of identifying where/why data contributes to their decision making

Level 1 Interfaces

- System – Threat Interface
- Threat – Target Interface
- Target – System Interface

APM Framework - Interfaces



APM Dynamic System Security Model

Existing Systems Dynamics Model

- Articulates the “arms race” between cyber attackers and cyber defenders
- Created using a high level of abstraction

State of System and Target Security

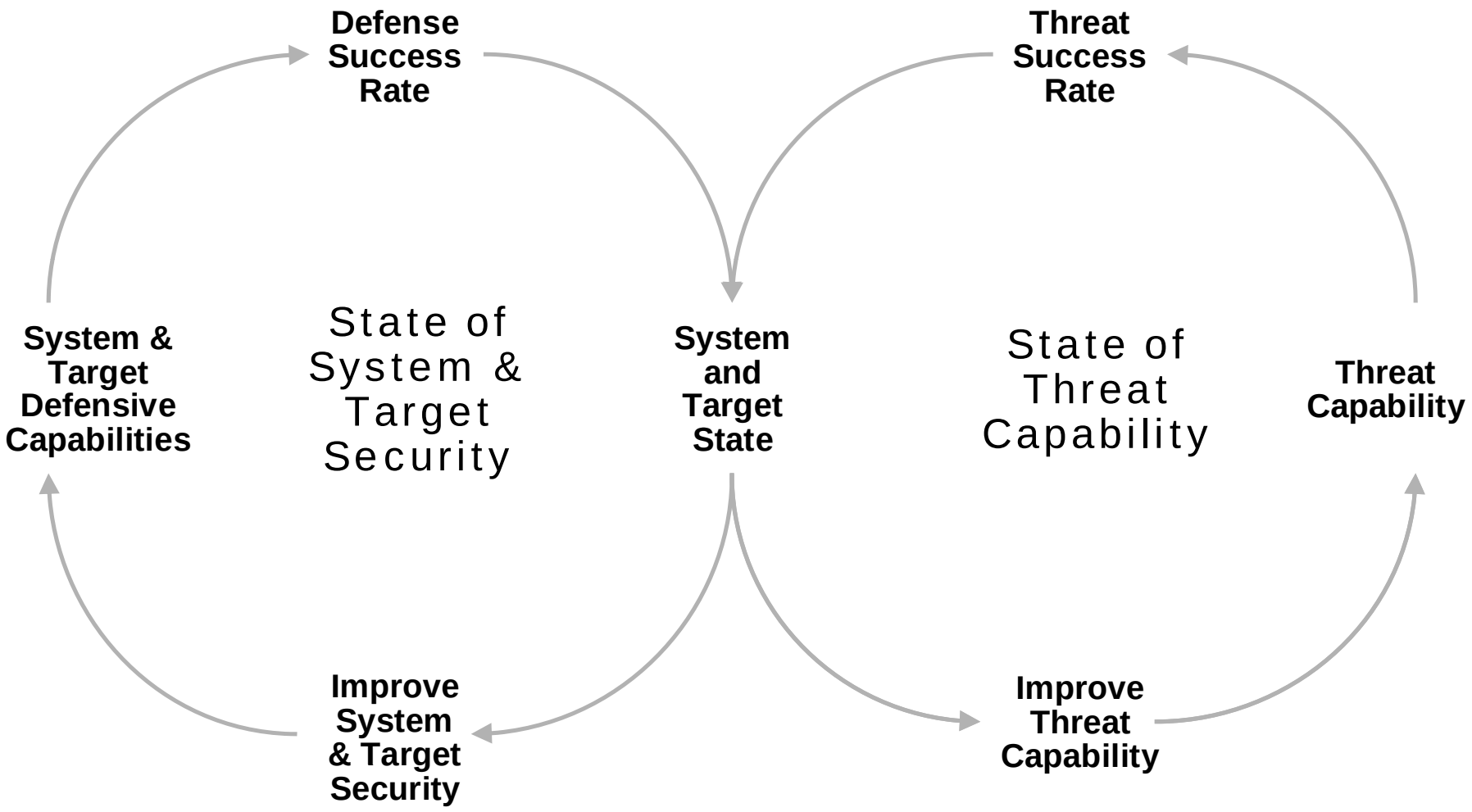
- System and Target Defensive Capabilities
- Defense Success Rate
- Improve System and Target Security
- System and Target State

State of Threat Capability

- Threat Capability
- Threat Success Rate
- Improve Threat Capability
- System and Target State

APM will provide the ability to build a more comprehensive dynamic systems security model

Dynamic System Security Model



Preliminary Results from Team Use (1 of 2)

Team objectives

- Understand the current state of cyber security incident reporting
- Determine the data quality associated with threat incident reporting
- Recommend methods for improved data quality collection

Asset Protection Model (APM) Application

- Used to organize a vast volume of existing data including:
  - Common Attack Pattern Enumeration and Classification (CAPEC)
  - Common Vulnerabilities and Exposures (CVE)
  - National Vulnerability Database (NVD)

APM Model Semantic Calibration

- Applied model to several standard non-cyber security threat instances
  - Bank robbery – threat actor, threat mechanism, threat vector
  - Car hijacking – threat actor, threat mechanism, threat vector
  - Terrorist attack – threat actor, threat mechanism, threat vector

Preliminary Results from Team Use (2 of 2)

Team APM Model Utilization

- Used to place incident data in context of cyber security
- Guided team judgments regarding applicability, quality of the data
- Supported analysis of information gaps and poor data quality

Team Results

- APM provided a structural context that could be analyzed by experts from a particular field
- Structure allowed communication of data between novice and experts
- APM viewed as effective
- APM provided structure needed to organize existing cyber security incident data
- Threat Cube concepts supported categorization, and definition of interrelationships between common threat types and attack patterns

Summary, Conclusions

The Asset Protection Model (APM)

- Establishes modules that allow internal controls, with communication and interaction at the interfaces
- Supports recursive definition of levels of abstraction
- Provides a focal point for the key asset protection communities – the IA, Systems, and Justice/Legal/IC
- Establishes a common framework for tailoring curriculum based on changes in technology and the threat spectrum
- Supports dynamic analysis of specific types of cyber defense activities
- Supports both human short-term cognition, and computer-enhanced reasoning methods
- Is independent of specific organizations and technologies, and will remain stable for an extended period of time

More Research Is Needed to Refine the APM Concepts, and Its' Applications

Questions???

Comments…