Is System Security Engineering Failing?

INCOSE International Workshop
Jennifer Bayuk
Cybersecurity Program Director
School of Systems and Enterprises
jennifer.bayuk@stevens.edu

V and V

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY

- **Verification**

  Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled.[ISO/IEC 15288].

  Did we build the system right?

- **Validation**

  Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. [ISO/IEC 15288].

  Did we build the right system?

Security Metrics History

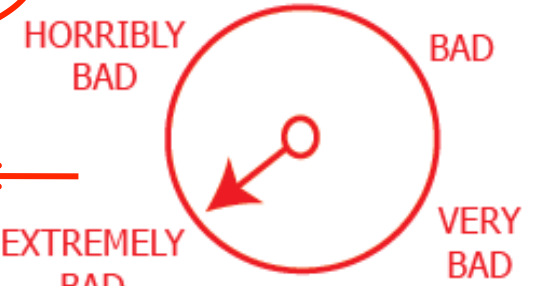
STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

- Orange Book
- Common Criteria
- Security Engineering Capability Maturity Model
- NIST Computer Security Handbook
- Recommended Security Controls for Federal Information Systems
- BS17799/ISO 27000 Series
- National Vulnerability Database

TTOA-centric

SDLC-centric

mgmt-centric



a badness-ometer

Security Analogies

STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY

- **Correctness and Effectiveness (C&E)**

  Internal to system development and operations

  Do the security features work?

  versus: Is the system secure?

- **Testing and Evaluation (T&E)**

  External to system development and operations

  Does the system meet certain criteria?

Variety in Security Metrics

Practical and useful:

"face validity"

- easy to connect to concept of security
- transparent data gathering process
- supports security decision-making

Not particularly:

- mathematical modeling of security management processes
- weighting network forensics evidence to increase probabilities of conviction
- quantifying threat surface using hidden Markov models
- using game theory to determine security investment strategies
- complex mathematical models for assessing software security

Typical Cost Justification

STEVENS INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

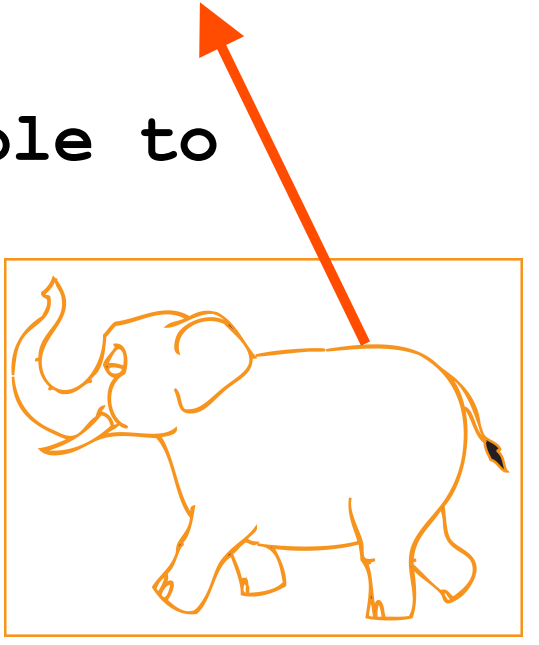
1. P = probability of event that causes harm

   C = cost of damage from the event

   T = cost of technology to prevent harm

2. P x C = amount it is reasonable to spend to prevent the event

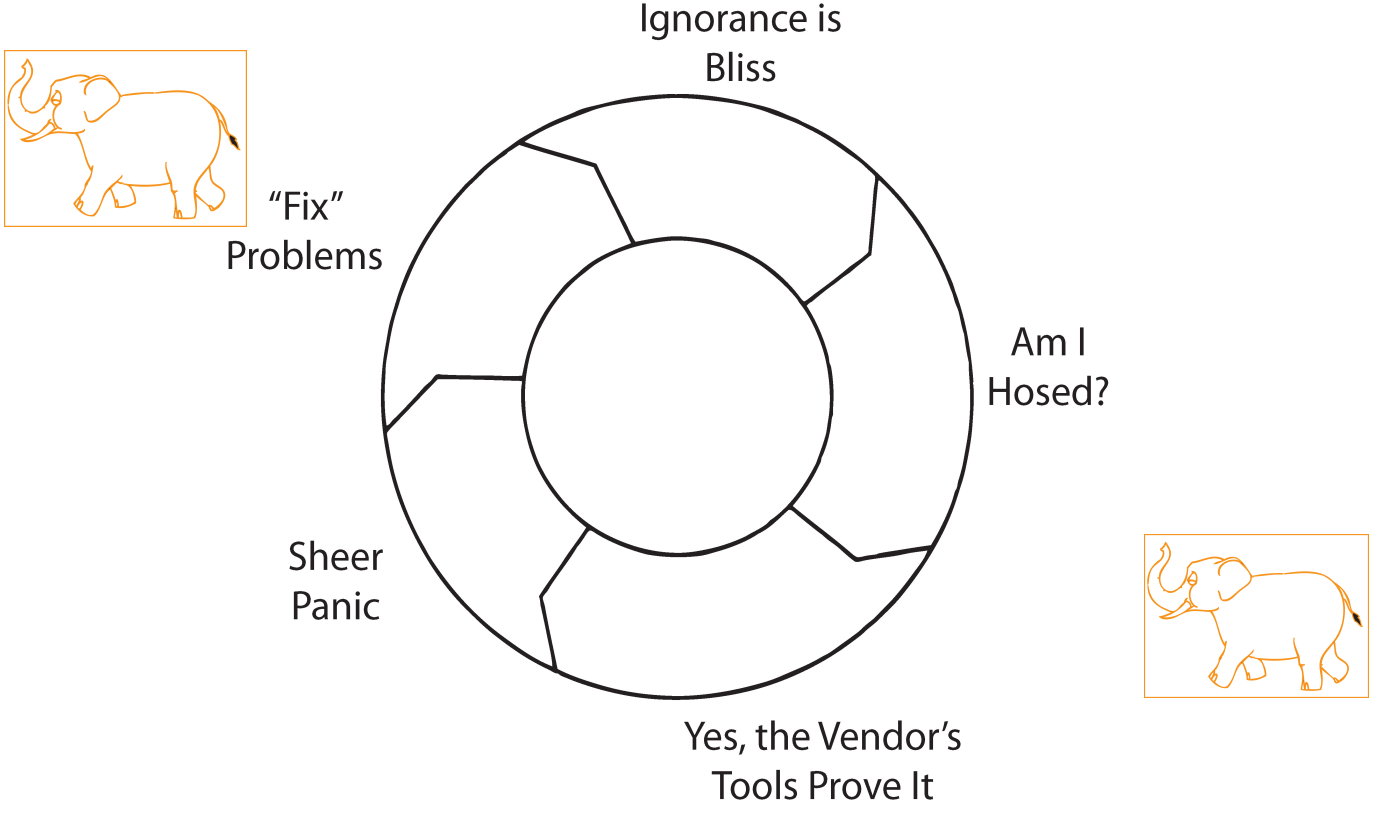
3. If (T < P x C), Buy T



Security Improvement Processes

The Hamster Wheel of Pain

An Alternative View of "Risk Management"



Source: Jaquith, Andrew, Security Metrics, Pearson Education, 2007.

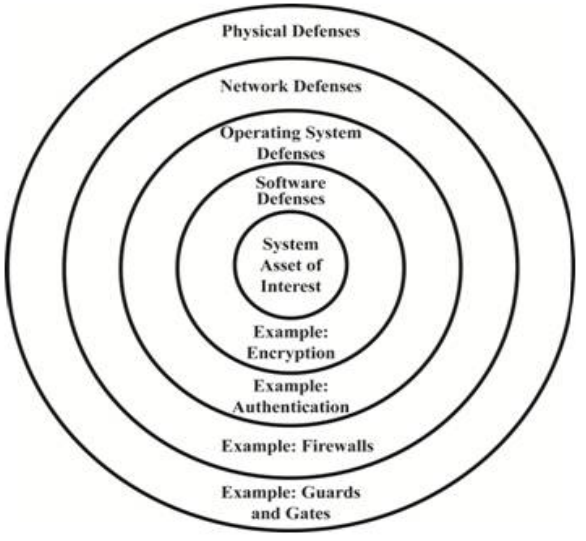
Model-based Approaches

Orange Book

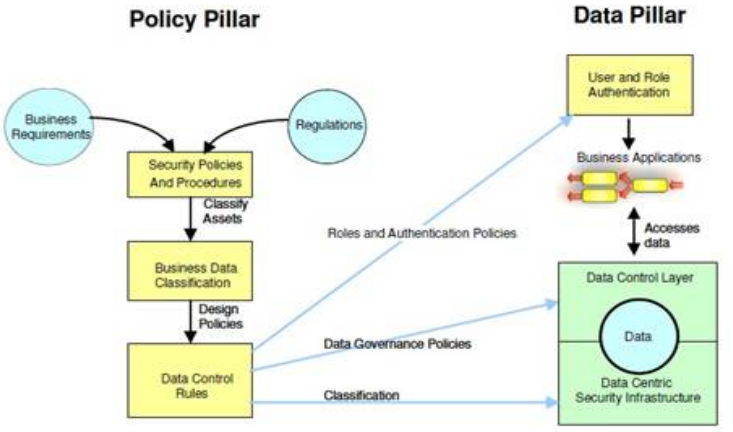
A1: Verified Design
B3: Security Domains
B2: Structured Protection
B1: Labeled Security Protection
C2: Controlled Access Protection
C1: Discretionary Security Protection
D: Minimal Protection

TRUST

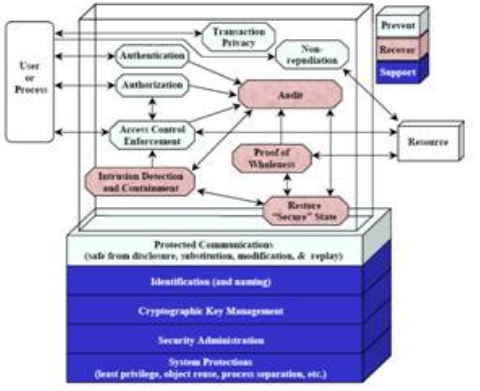
Defense in Depth



Data Centric



Security Services



Security Functional Overlap

STEVENS Institute of Technology

System	Overlap	Security
Sensor-enabled Monitoring	Data Continuity	Confidentiality
Telecommunications	Protocol integrity	Bandwidth utilization forensics
Financial Services	Identity management	Transaction Audit
Military	Confidential communications	Recovery and Reconstitution
Industrial Control	Incident detection and recovery	Protection against insider threat
SmartGrid	Accountability	Theft and Fraud investigation
Airspace	Situational Awareness	Software integrity
Cyberspace	Software integrity	Privacy

A Systematic Look at Security

Security:	**Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.**
Security Feature:	**A system capability that contributes to its security.**
Security Metric:	**Measurement that characterizes an attribute of the system of interest that is proposed to have both face and construct validity in the context of a hypothesis that the system is secure.**
Security Framework:	**The concept of operations, mission, and environment under which a system operates.**

A Systemic Approach

SYSTEMS ENGINEERING
Research Center

- Clear framework statements
- Thorough threat environment description
- Clearly defined solution criteria
- List of solutions in the form of security features
- Proposed hypothesis formulated to shed light on each solution and how it may be proven or disproven
- Verification and Validation metrics
- Summary of results

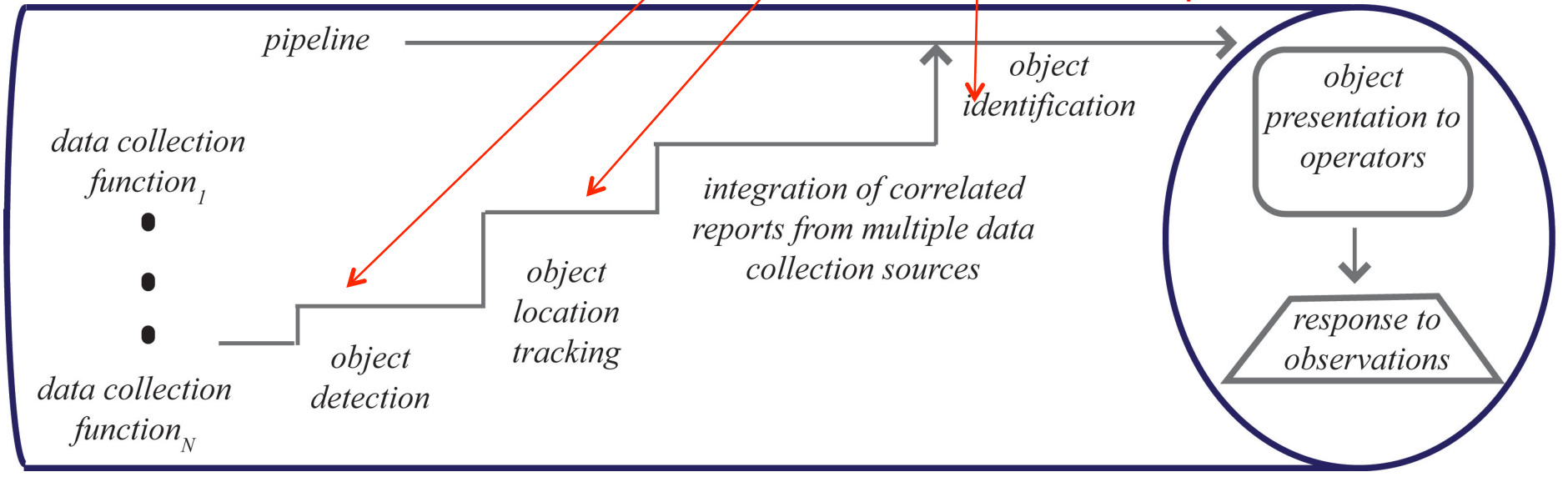
Frameworks

- Patterns at system level
- Security is identified with resiliency of mission
- Systemic security features are functional requirements
- Architecture security metrics verify and validate functional requirements

Possible Functional Security Metrics:

- sensor signal-to-noise ratios
- data integrity cross-platform checks
- the type and number of information delivery alternatives available to the end user/operator

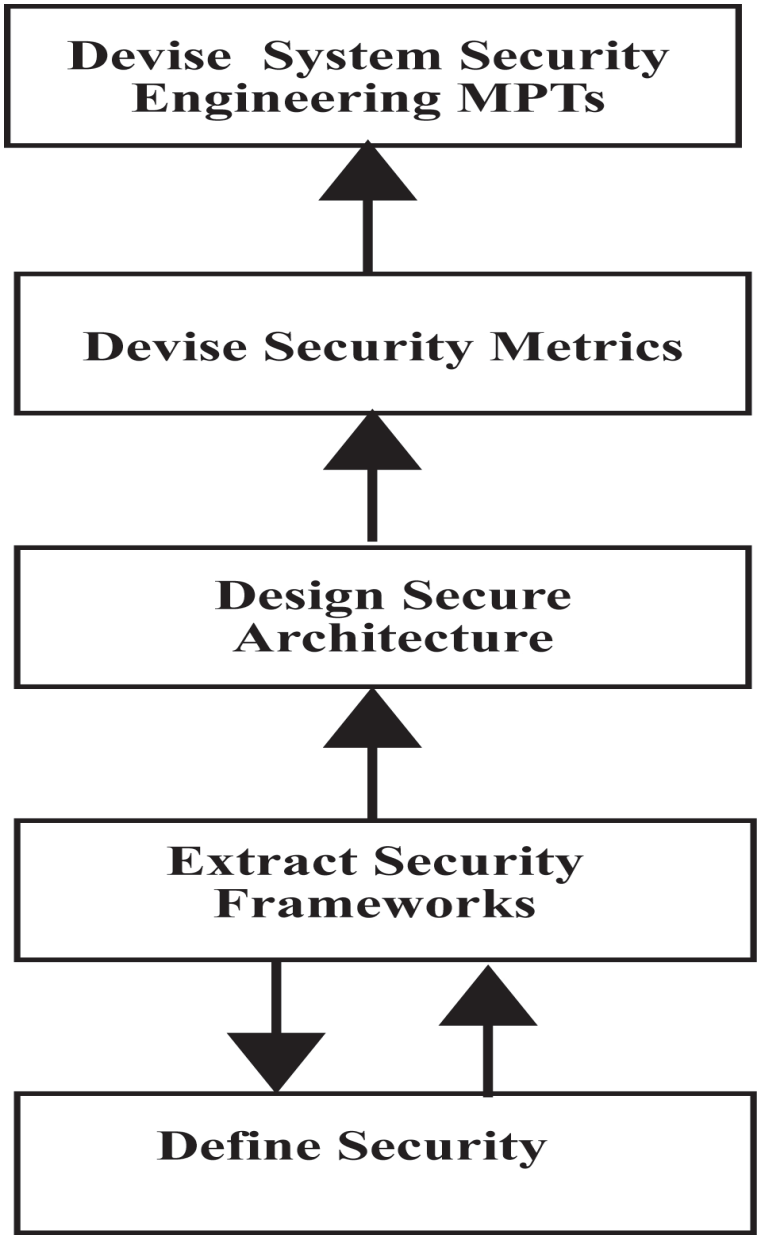
Example: Pipelined monitors



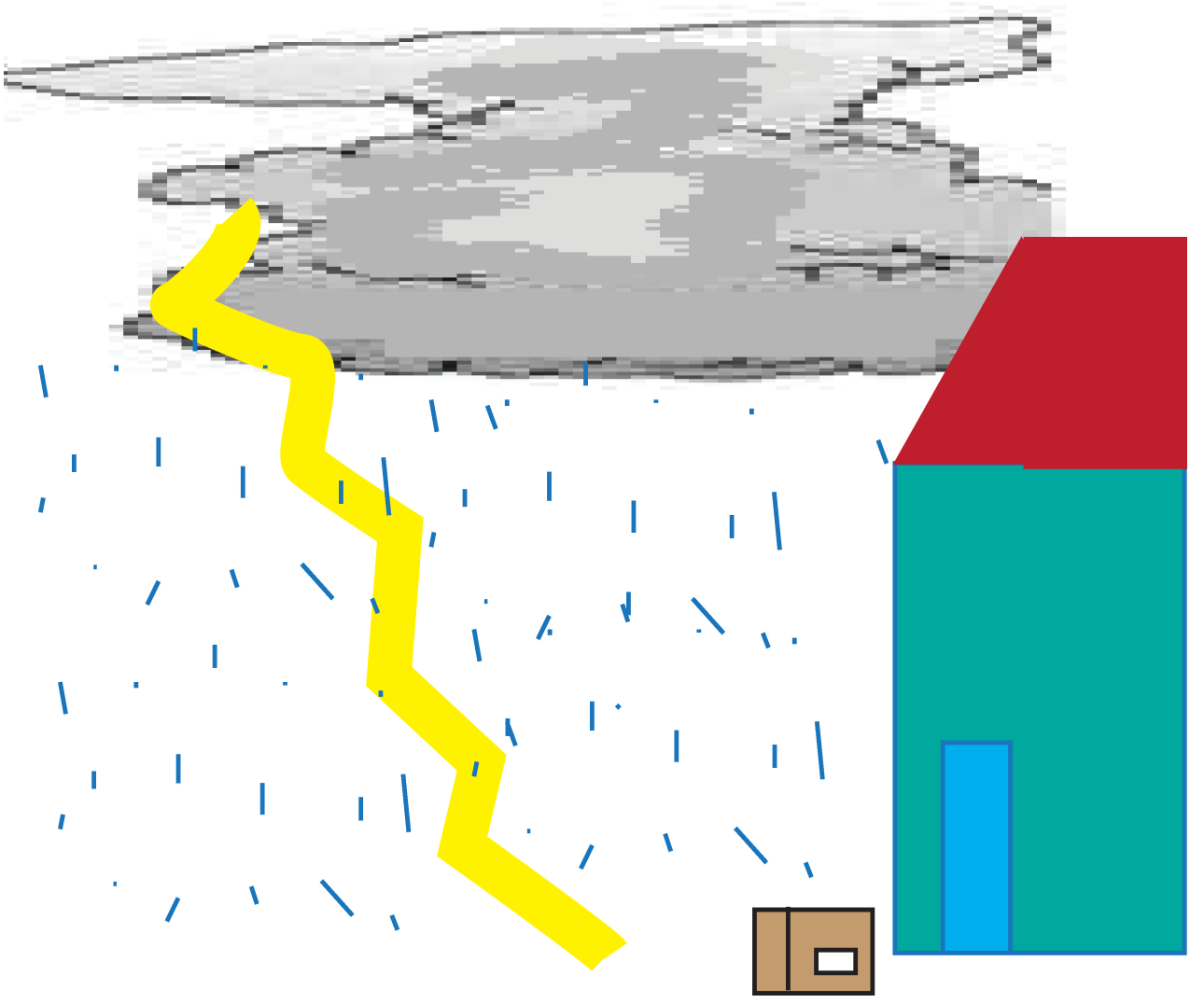
Source: Bayuk and Horowitz, An Architectural Systems Engineering Methodology for Addressing Cyber Security, Systems Engineering, 2011

New Security Methodology

SYSTEMS ENGINEERING
Research Center



Weatherproofing Analogy



Source: Bayuk, Enterprise Security for the Executive, 2010

Security V&V

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY

Questions? Discussion…

jennifer.bayuk@stevens.edu