Mission Aware Cybersecurity

Cody Fleming (UVA)
Scott Lucero (OSD)

Peter Beling, Barry Horowitz (UVA), Calk Elks (VCU)

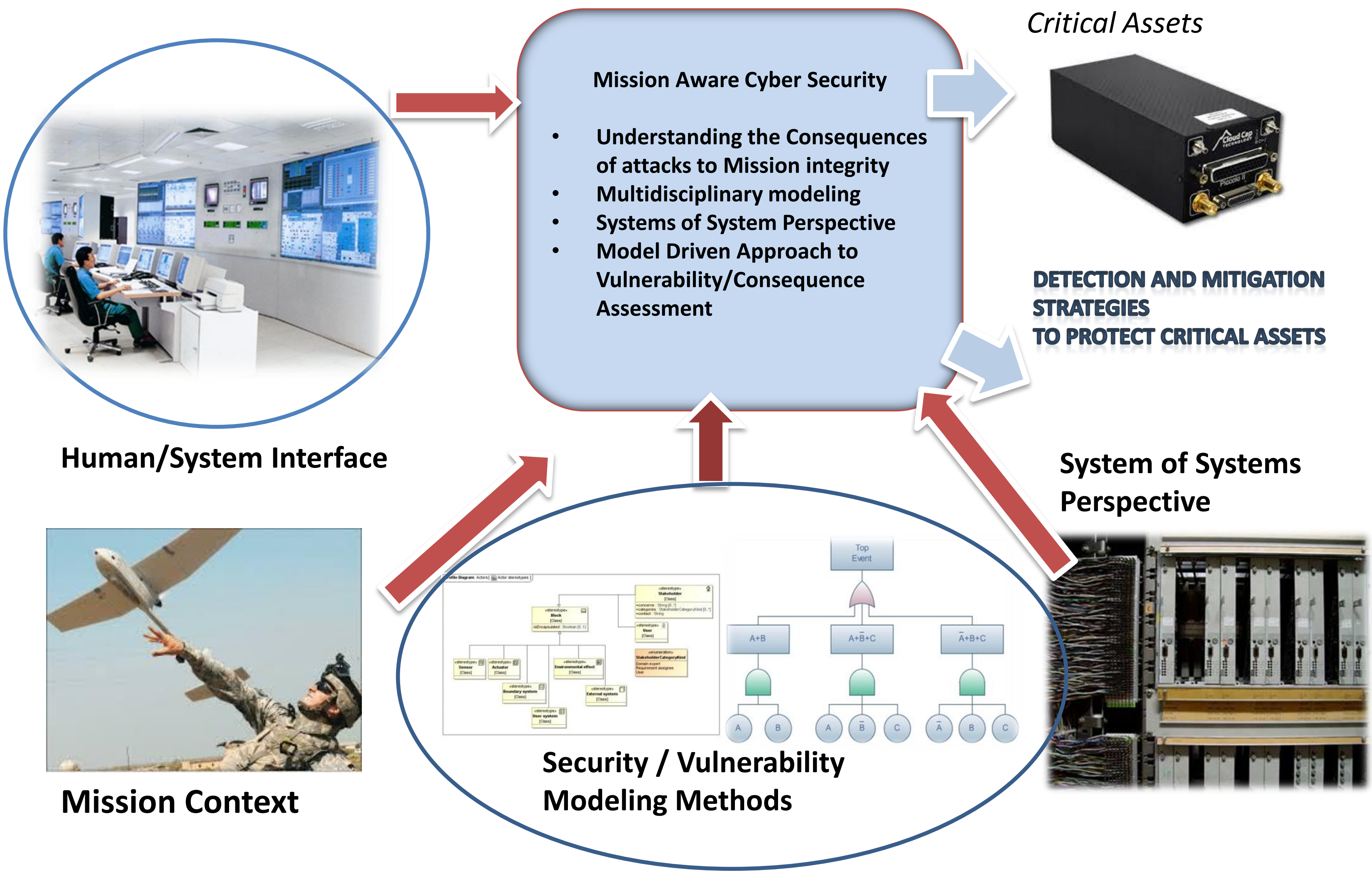
October 2016

Systems Engineering Research Center (SERC) Overview

- DoD and the Intelligence Community established the SERC University Affiliated Research Center (UARC) in September 2008
  - Long term, strategic relationship for systems engineering research
    - Free from organizational conflicts of interest
  - Vision: "The *networked* national resource to further systems research and its impact on issues of national and global significance."
  - Five year contract with Stevens Institute and 22 collaborating universities renewed in September 2013
- ASD(R&E) and the Intelligence Community are the original sponsors
  - Defense Acquisition University, Army, Navy and Marine Corps now also sponsor research
- SERC awarded more than $55M for systems engineering research
  - $5M core funding for Engineering Science and Technology, starting in FY14
  - Research organized in four thrusts
    - SE Transformation, Trusted Systems, SoS, Human Capital

SERC Collaborating Universities

Mission Aware Cybersecurity



Mission Aware Cybersecurity: An Approach to Resiliency for Physical Systems (1 of 2)

- Response to attacks that penetrate network and perimeter security defenses
- Also insider and supply chain attacks
- Application domains:
  - Weapon Systems
  - C2 Systems
  - Sensor Systems
  - Logistics Systems
  - Computer Controlled Physical Systems (Engines, Electrical Power, Rudder Control)
  - Etc.

Mission Aware Cybersecurity: An Approach to Resiliency for Cyber Physical Systems (2 of 2)

- Securely monitor physical systems for illogical control system behaviors (Secure Sentinel technology)
- For detected attacks:
  - Inform system operators
  - When possible, provide decision support for reconfiguration

- Developed, and currently developing, a number of prototype solutions including evaluations of responses to cyber attacks during system operation

  - UAV Surveillance system (DoD)
  - 3D Printer (NIST)
  - State Police cars (Virginia)

  Completed Efforts

  - Radar(DoD)
  - Tank Fire Control System(Picatinny Arsenal)
  - Navy Ship (SBIR Partnership)

  Started Efforts

Illustrative Examples of Illogical Control

- Navigation waypoint changed, but no corresponding communication received by UAV
- Automobile sensor shows distance between cars reducing, but collision avoidance control system speeds up the following car
- Selected material to create part of a 3D printed object does not match what the executing design calls for
- Mode of Fire Control System changed, but no touch screen input from operator

A Set of Techniques Utilized in System-Aware Security

<u>Cyber Security</u>

* Data Provenance
* Moving Target

  (Virtual Control for Hopping)
* Forensics

<u>Fault-Tolerance</u>

* Diverse Redundancy

  (DoS, Automated Restoral)
* Redundant Component Voting

  (Data Integrity, Restoral)

<u>Automatic Control</u>

* Physical Control for Configuration Hopping

  (Moving Target, Restoral)
* State Estimation Techniques

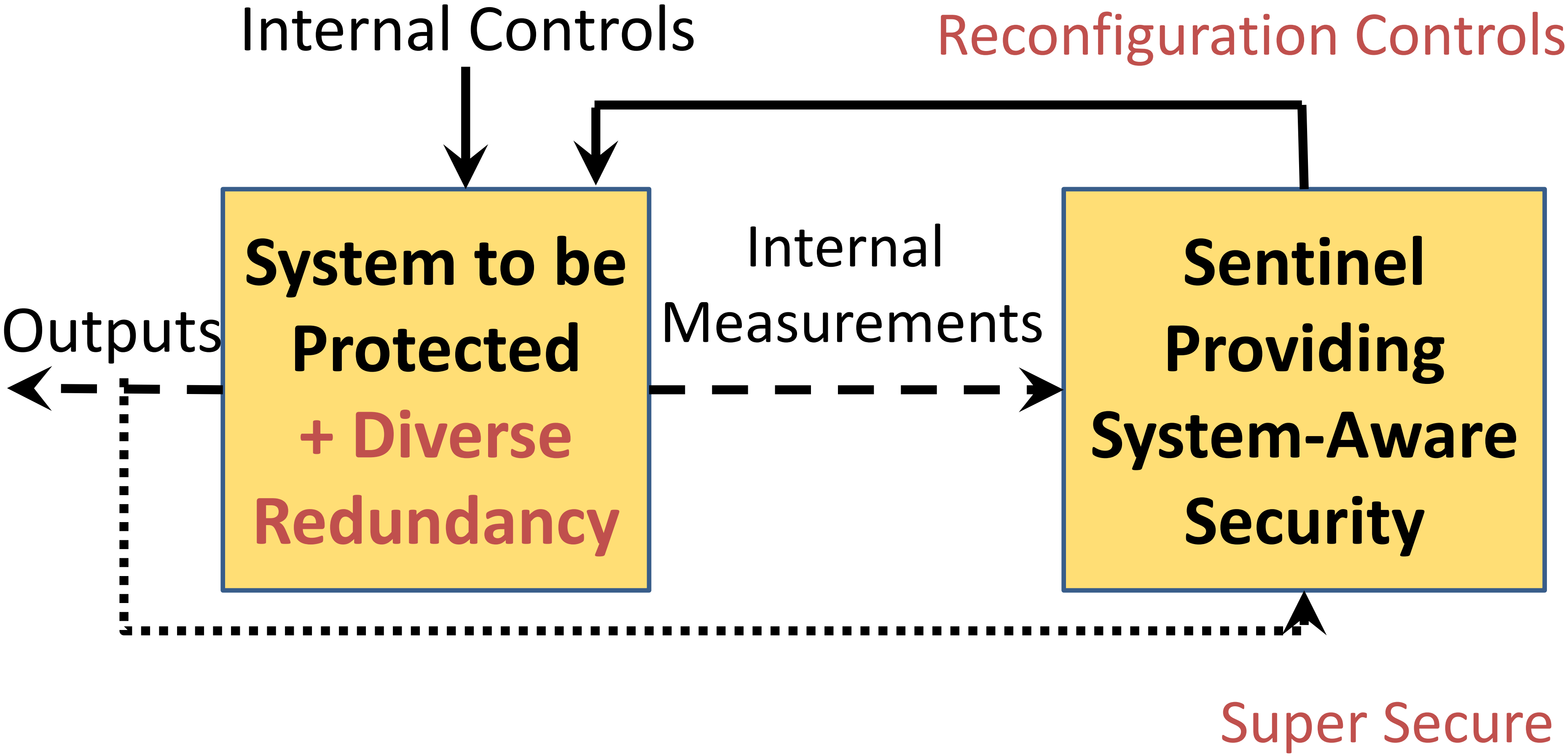
  (Data Integrity)
* System Identification

  (Data Integrity, Restoral)

This combination of solutions requires adversaries to:

- Understand the details of how the targeted systems actually work
- Develop synchronized, distributed exploits consistent with how the attacked system actually works
- Corrupt multiple supply chains

High Level Architectural Overview



Architectural Assessment & Selection Process

- **Identify Relationships between sub-systems, functions and variables**

  What is critical to protect?
- **Recognize the Possible Paths an Attacker Could Take to Exploit critical sub-systems..**

  What are the opportunities for and consequences of attacks?
- **Determine the Subset of Attack Actions Most Desirable to an Attacker.**

  What is exploitable and by whom?
- **Identify appropriate defensive actions and their impacts on the attacker**

  Pre-selection of cyber defenses
- **Evaluate the impacts of the selected cyber-defensive actions on the system.**

  What does this cost me and can I afford it?
- **Weigh the Security Trade-offs to Determine Which Architectural Solutions Best Reverse the Asymmetry of a Potential Attack.**

  Effectiveness of best solutions

Modeling Tools for Accuracy at Scale

- **Systems Models** to capture the relationships between functional system entities and to recognize patterns (data, dependence, control) within the system.
  - Be able to represent the system attack surface (danger of under modeling) .
  - Represent the initial system "as-is" with minimal defense and again with possible security solutions implemented.
  - Value in showing solutions integrated into the holistic system for context.
  - Used to model an understanding of the complexity added to an attack by particular defenses.
  - Initial approach used influence diagrams. Currently developing a suite of tools in SysML.
- **Attack Trees** to identify possible paths an attacker could take to exploit the system.
  - Uses assessments of the attack actions and the attackers' capabilities to determine the subset of most preferable actions.

Outcomes and Objectives from Initial Studies

- Need methods to support information gathering from operational community and semi-automatically convert into SysML models
- More systematic methods for accounting for historical attack information in the vulnerability assessment process

Towards Automation Support for Vulnerability Assessment

- Expressing mission requirements in terms of low level requirement properties (e.g. platform security properties)
- Gathering pertinent threat and historical attack information (special databases, CAPEC)
- Finding attack patterns that are potentially "productive" against our system … Difficult search problem

From Mission Requirements to Systems Models & Properties

Mission Domain – What are all of these integrated systems trying to achieve for us?

Functional Domain – How do we describe operational and function behavior, input/output, state interactions – accurately

Architecture Domain – How are all of the Platforms/sub-systems organized, connected, and related to each other to achieve mission objectives

Platform domain –What are the Platform functions providing or requiring in the context of mission

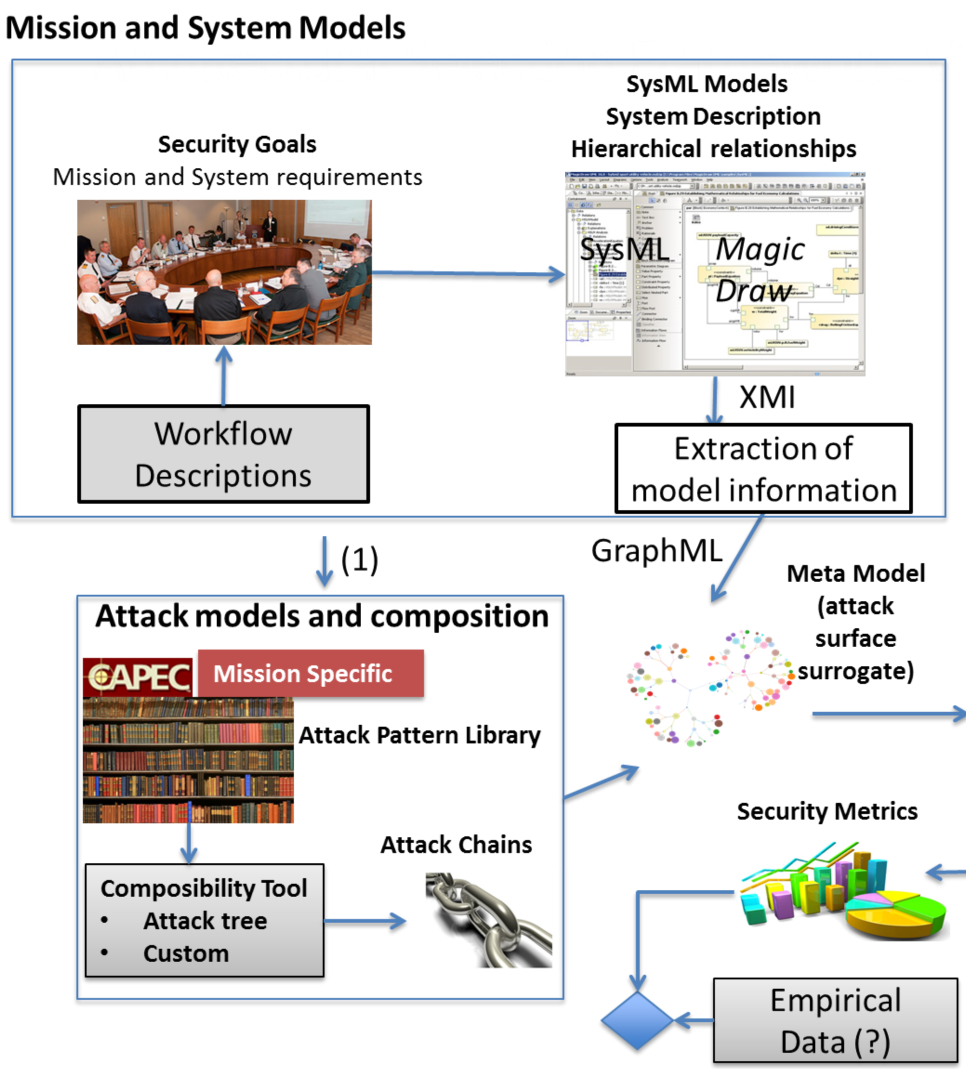
Increasing levels of detail

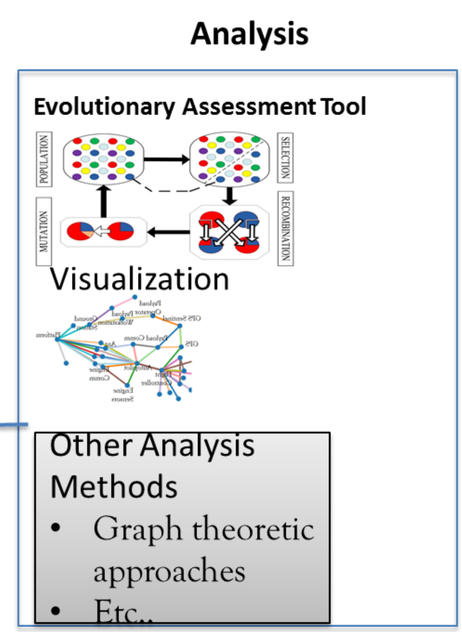
- Support decision making by providing model based reasoning along these dimensions
- Provide a models to collect insight that otherwise could be overlooked
- Integrate Exploit Tools (Attack Trees) to the framework
- Be able to access the criticality of platforms and functions with respect to mission
- Evaluate cyber-defenses

Mission Aware Tool Framework

<u>Tool based Paradigm</u>

- Support exploration – Diverse Analysis
- Separation of concerns – analysis vs modeling
- Low threshold – easy entry
- High Ceiling - can be used by experts
- Open Ecosystem support - Use community supported tools, languages





Outlook

- Continue development of architectural selection tools
- Case studies with military partners
  - Design of defensive architecture
  - Implementation of attacks and defenses
- Trust and systems operations
  - Sentinels or operators take control if trust in system is lost
  - Tradeoff between risk and mission capability