The Science of Cyber Security

Laurie Williams
williams@csc.ncsu.edu
NSA Science of Security Lablet (SoSL)

• NSA SOSL lablets:
  – North Carolina State University (Analytics)
  – Carnegie Mellon (Scalability, Usability)
  – University of Illinois (Resiliency)

• Projected $2.0-$2.5M funding per year per lablet

• NCSU: Based out of Computer Science
  – 14 supported NCSU faculty; 18 supported NCSU students
  – Multi-disciplinary: 3 NCSU colleges and institutes
  – 5 collaborating university partners
Hard Problem 1: Scalability and Composability

Challenge

• Develop methods to enable the construction of secure systems with known security properties.

Hard Problem 2: Policy-Governed Secure Collaboration

Challenge

• Develop methods to express and enforce normative requirements and policies for handling data with differing usage needs and among users in different authority domains
Hard Problem 3: Predictive Security Metrics

Challenge

• Develop security metrics and models capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically), in a given context.
Hard Problem 4: Resilient Architectures

Challenge

• Develop means to design and analyze system architectures that deliver required service in the face of compromised components

http://thecybersaviours.com/intrusion-detection-system-ids
Hard Problem 5: Human Behavior

Challenge

• Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties