University of Idaho
College of Engineering

HESTIA: High-level and Extensible System for Training and Infrastructure risk Assessment

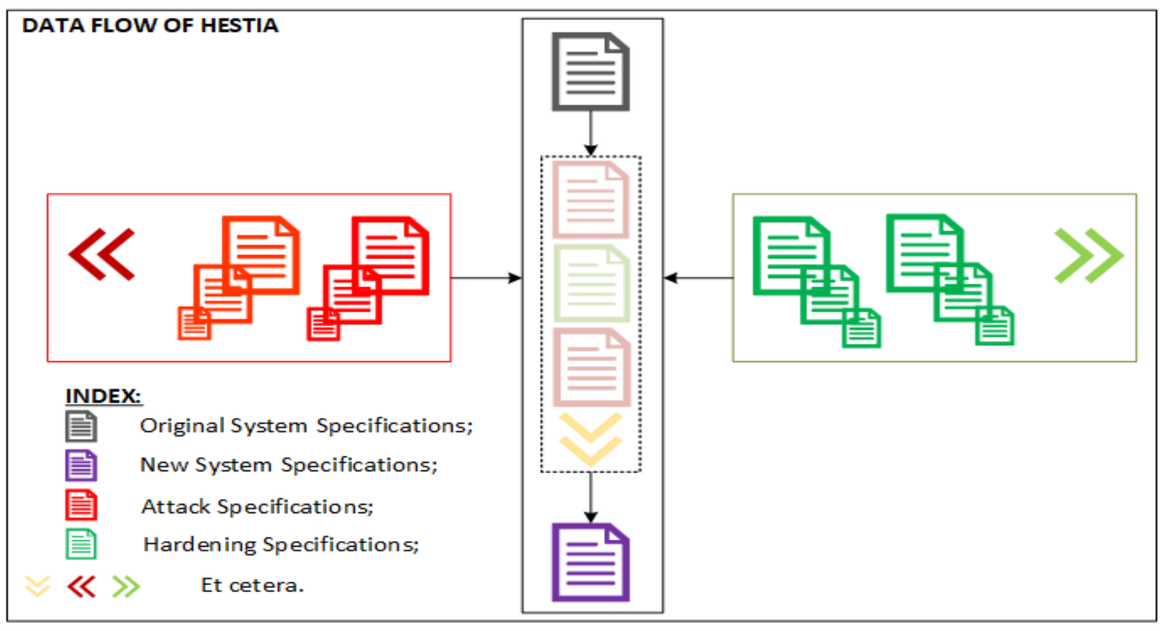
GOALS

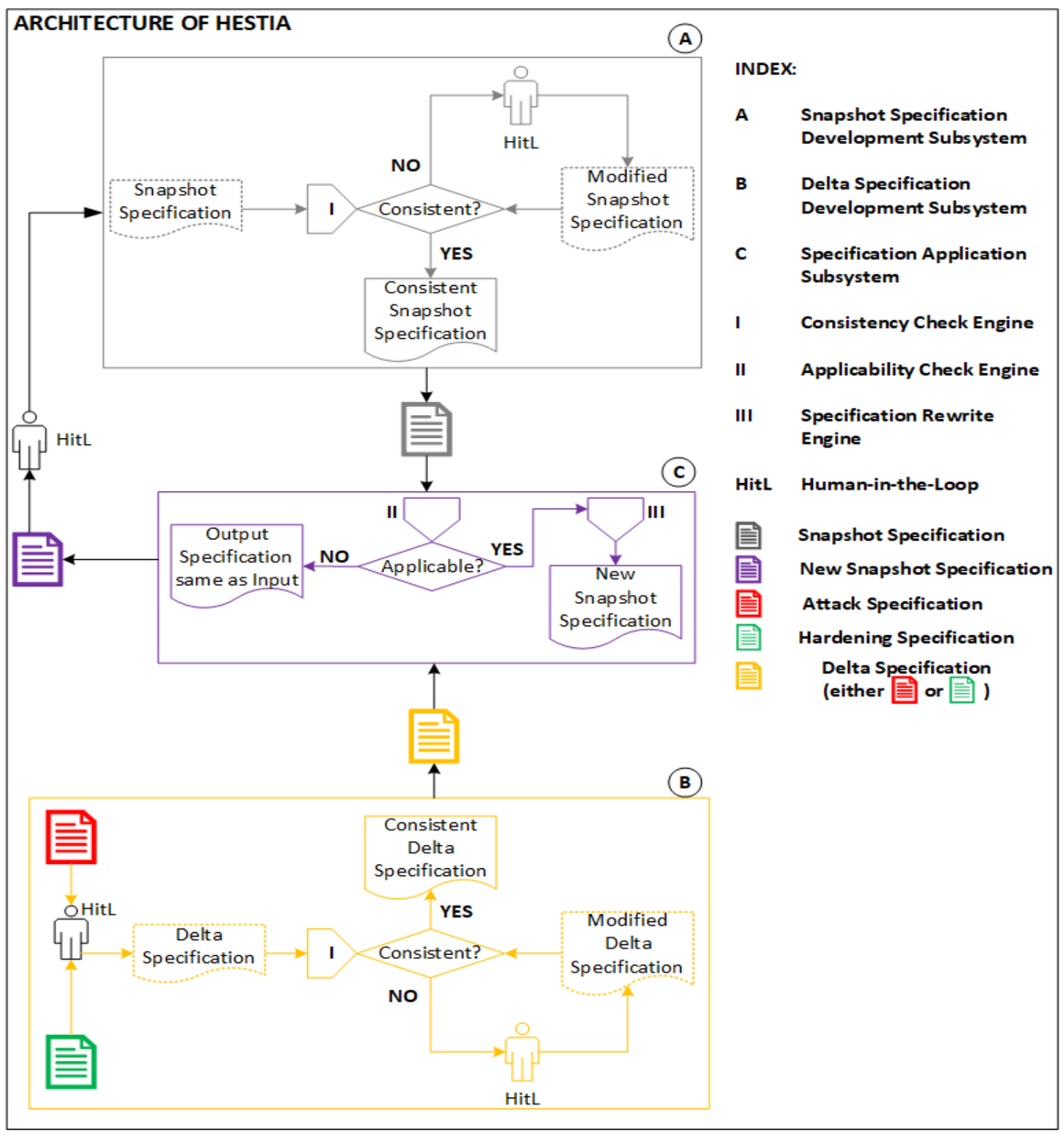
- Concretely identify the basis of risk abatement so that, as the CPCS-infrastructure and subsequently, the attack surface evolves, we can iteratively ensure that no new vulnerabilities have been introduced;
- Enable the guided execution of attack-defense scenarios for infrastructure risk assessment and training;
- Train CPCS-infrastructure managers in foreseeing potential attacks and implementation of respective defenses;
- A high-level, complete, rigorous, consistent, and iterative process-oriented system that subjects a CPCS infrastructure's security specification to attack-defense specifications (i.e., scenarios or test cases).

PROBLEMS BEING ADDRESSED

- A Chief Security Officer (CSO) should be able to design the best hardening strategy for their particular CPCS-infrastructure.
- Such an analysis includes investigating questions along the lines of: "where to best use defense resources, which parts to harden, and in which particular order?"
- Several factors come into play in such an investigation: completeness and consistency of the CPCS infrastructure policies, likeliness of attacks and respective defenses against the particular system, and overall cost of possible attacks vs. overall cost of possible defenses.
- We use the term overall cost to denote cost in both: money and time.

DATA FLOW AND ARCHITECTURE





INTENDED WORKING OF HESTIA

- When fully developed, HESTIA will be able to:
  - Take an existing CPCS infrastructure's specification file as input, check it for consistency and produce a consistent specification.
  - Take the consistent specification and identify the type of attacks or defenses, which can be applied on the CPCS infrastructure, thereby changing the specification.
  - These changes occur in the form of applicable attacks and/or hardening specifications resulting in transformation of an original system specification into a new system specification.
  - The new system specification can then be subjected to another iteration of the same process, as determined by a human supervisor.
  - For every iteration, either an attack or a hardening specification is chosen by a human supervisor from a pre-compiled library of attack and hardening specifications.
  - This library of attack and defense specifications is compiled by human(s) as well.
- HESTIA can conduct this assessment iteratively, until a human supervisor stops the process.
- This assessment data can then be used by a CSO, to prepare the best hardening strategy for their particular CPCS infrastructure.

CURRENT RESEARCH STATUS

- We have designed and developed a prototype language for high-level CPCS infrastructure policy specification.
- The language is called as HERMES: High-level, Easily Reconfigurable Machine Environment Specification.
- Some characteristics of HERMES are:
  - High-level and easily reconfigurable policy specification language.
  - Can specify domain information like groups, sub-groups, users, roles, and devices.
  - Can specify policy information like parent, target, status, field and rationale.
  - Independent of any particular application and platform, i.e., an operating system.

FUTURE WORK

- Design and develop case studies, reflecting deployment of CPCS infrastructure in real world. We plan to design and develop at least two such case studies. We also plan to use HERMES as the specification language to represent the state of case studies' CPCS infrastructure.
- Research on possible infrastructure, attack, and hardening measures' specification completeness and inconsistencies. Subsequently, design a series of algorithms for consistency checking.
- Develop a library of attack and hardening measures-based specifications. These attacks and hardening specifications should ideally be modeled after real world possibilities or at least, as close to real world as possible.
- Investigate the modalities of applying the attack and hardening measures on a CPCS infrastructure. Design a series of algorithms for applicability checking.
- Create a rewriting engine, which rewrites a snapshot specification, by applying the aspects of an attack or hardening specification.
- Develop a proof-of-solution for the HESTIA architecture, by incorporating result of all the above mentioned agenda items.

CONTACT INFORMATION

Ananth Jillepalli
Doctoral Candidate, Cybersecurity
Center for Secure and Dependable Systems,
University of Idaho.

E-Mail: **ajillepalli@uidaho.edu**

DEPARTMENT OF COMPUTER SCIENCE | CENTER FOR SECURE AND DEPENDABLE SYSTEMS | UNIVERSITY OF IDAHO
THIS PROJECT'S FUNDING SUPPORT IS PROVIDED BY THE STATE OF IDAHO UNDER IDAHO GLOBAL ENTREPRENEURIAL MISSION (IGEM) GRANT OF 2016