The Center for Cyber Defenders

Expanding computer security knowledge

SAND2016-6738C

Fundamental Trust Analysis

Modeling Supply Chain Security

Greg Walkup, Baylor University;
Nathan Burow, Purdue University

Project Mentor: Brandon Eames, Org. 5638

Problem Statement:

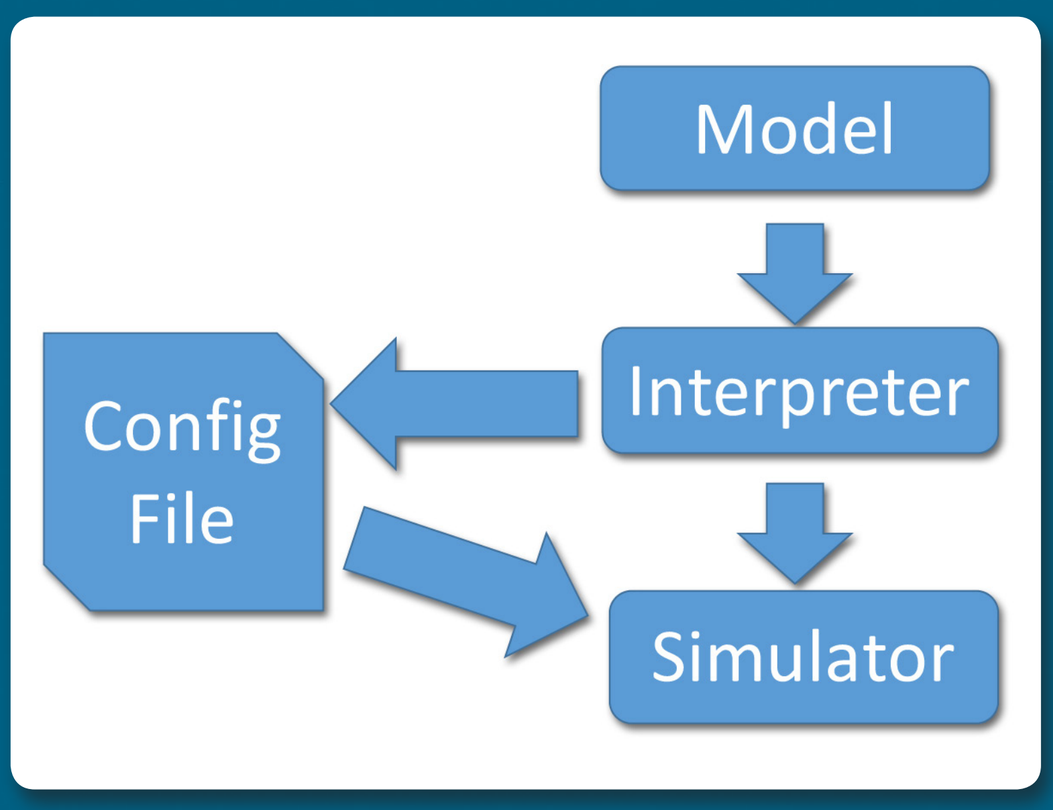
Computing in sensitive applications requires trusted hardware. A subtle adversary can attack the supply chain of a trusted system for malicious purposes. Modeling attacks on supply chains and simulating their probability allows us to quantitatively assess vulnerabilities and implement effective mitigations.

Objective and Approach:

- Generic Modeling Environment(GME)
  - Allows creation of domain-specific modeling languages
  - Used to create a supply chain modeling language (SCML) for modeling attacks on supply chains
- Attack Graphs
  - Are composed of operations an adversary could perform
  - Supply chain and attacks are modeled independently
- Simulation
  - Takes an attack graph as input and evaluates each attacker and defender strategy
  - Determines the highest-risk attacker strategies and allows selection of mitigation approaches

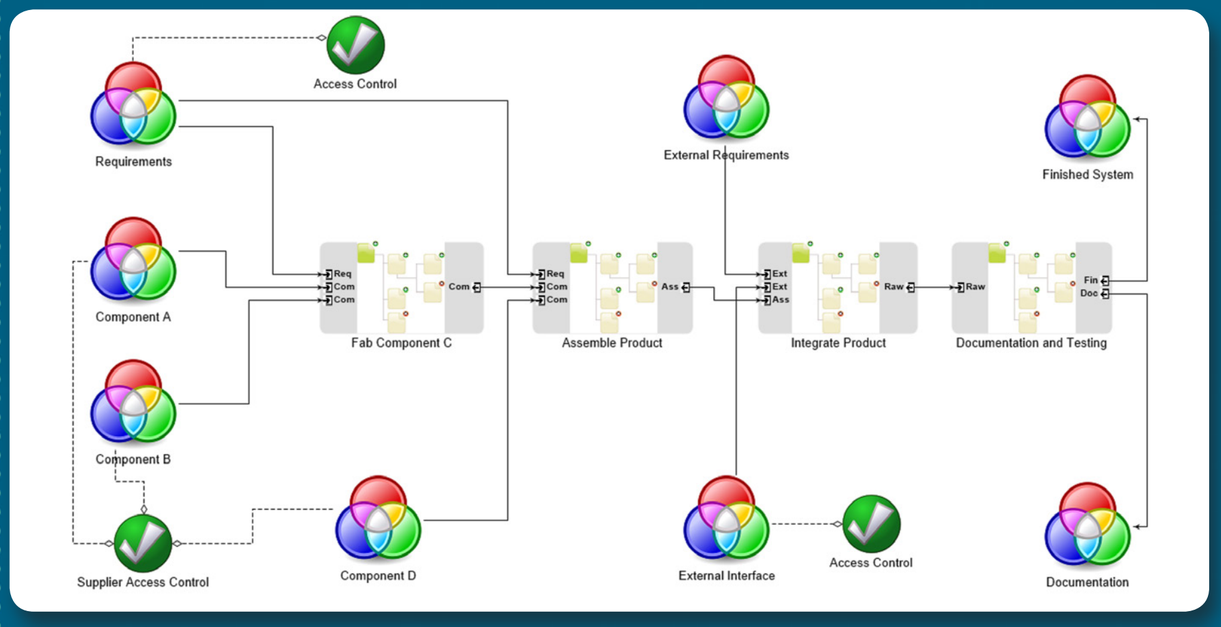
Results:

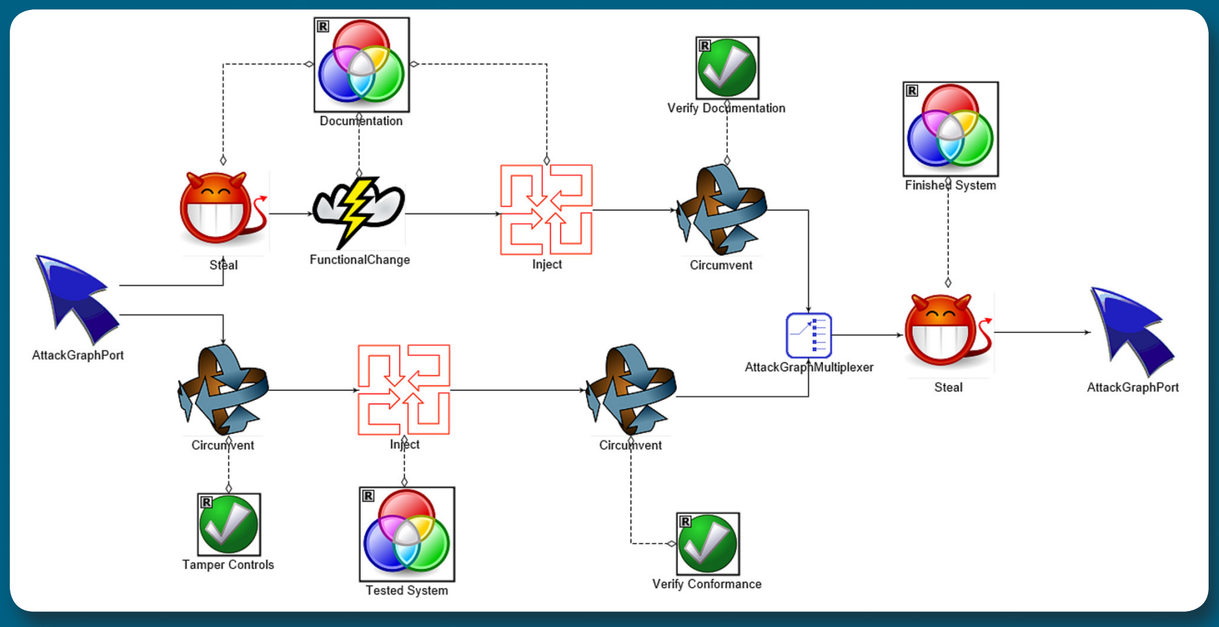
- Advanced the SCML modeling language to incorporate well-defined semantics for families of related attacks
- Developed a model interpreter capable of generating configuration files for the simulation tool based on an attack graph
- Prototyped a simulator implementation that can produce quantitative trust analysis results based on game theory



Impact and Benefits:

- Facilitates exhaustive mathematics-based analysis of system trustworthiness
- Allows stakeholders across Sandia and the US Government to quantify the risk of fabricating trusted hardware instead of assuming trust





Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-84AL8500. SAND2016-XXXXC.