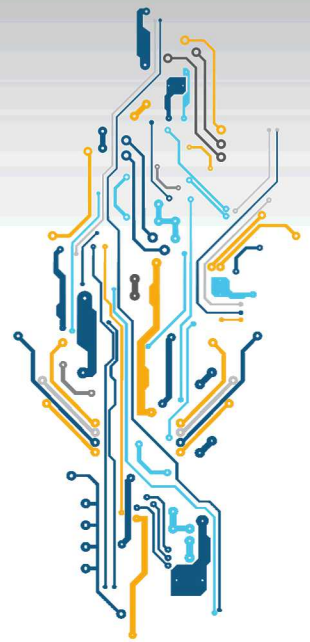
SAND2020-5199C



On the Risk of Development-Time Subversion

Brandon Eames, PhD
Sandia National Laboratories
bkeames@sandia.gov

CReSCT
Cyber Resilient Supply Chain Technologies
2020 Virtual Workshop

Idaho National Laboratory

IEEE

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

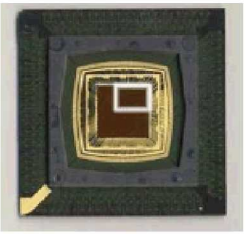
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Project GUNMAN

- Based on a tip from another government, in 1984 the US Government quietly and quickly replaced 10 tons of electronic equipment in the US Moscow embassy
- Subsequent evaluation of replaced equipment revealed a sophisticated bug in a small number of IBM Selectric typewriters

Assurance in Microelectronics-Based Systems

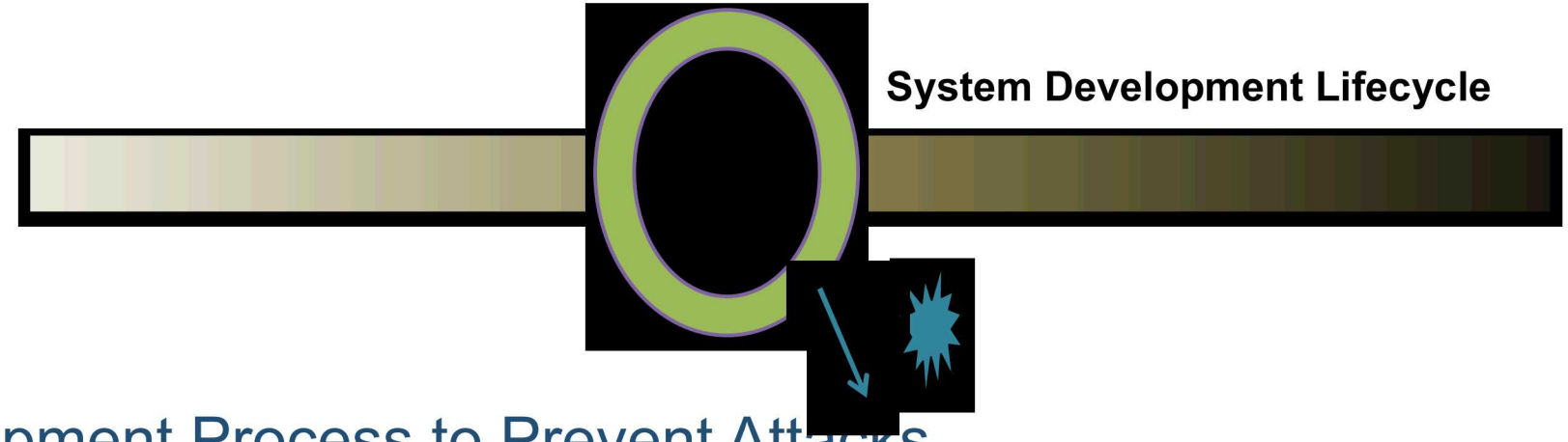



- Society relies on microelectronics-based systems for safety, security, entertainment, travel, etc.
  - Internet, satellite systems, transportation, cyber infrastructure, critical infrastructure (e.g. power grid), cloud, communications, health care, etc.
- Can adversaries manipulate these systems prior to their deployment? What would the impact be?
- Can these systems be ***trusted*** to perform their intended function?

How vulnerable are systems to development-time manipulation?

Current Approach to Trusted System Development

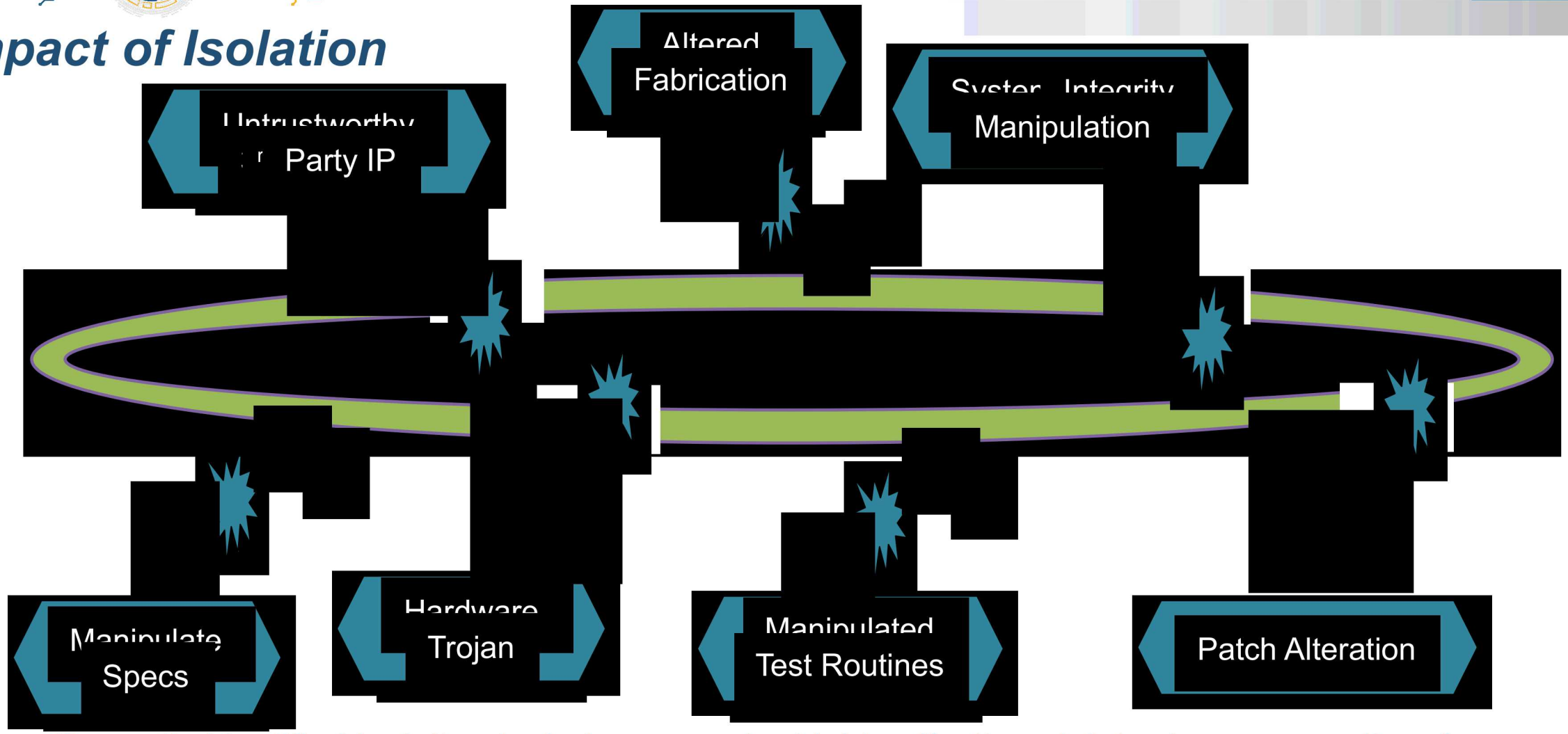


Isolate Development Process to Prevent Attacks

- Keep the attacker from manipulating the system / development process
- Process-based approaches: control information flow, control supply chain, isolated manufacturing etc.

- Examples:
  - US Government's **Trusted Foundry Program**: certification process to establish isolated microelectronics fabrication
    - Ensure integrity, availability of microelectronics fabrication
  - Isolated computer networks
  - Vetted design teams

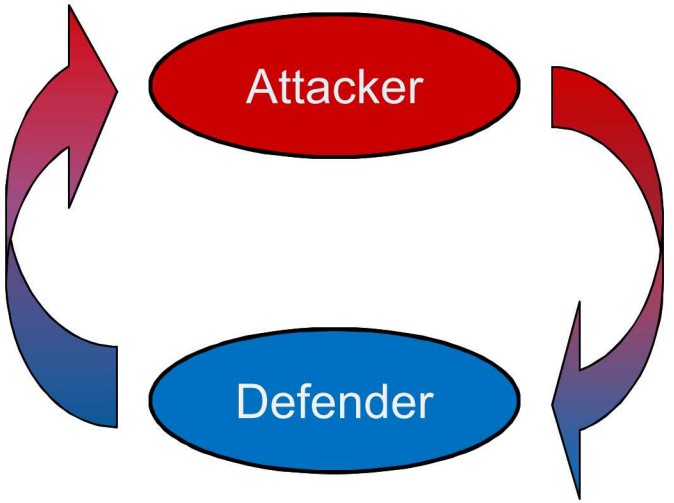
Impact of Isolation



- Currently identified isolation techniques can be highly effective at deterring many paths of adversary access
- ***Gaps Remain: Practicality of real system development precludes complete isolation***

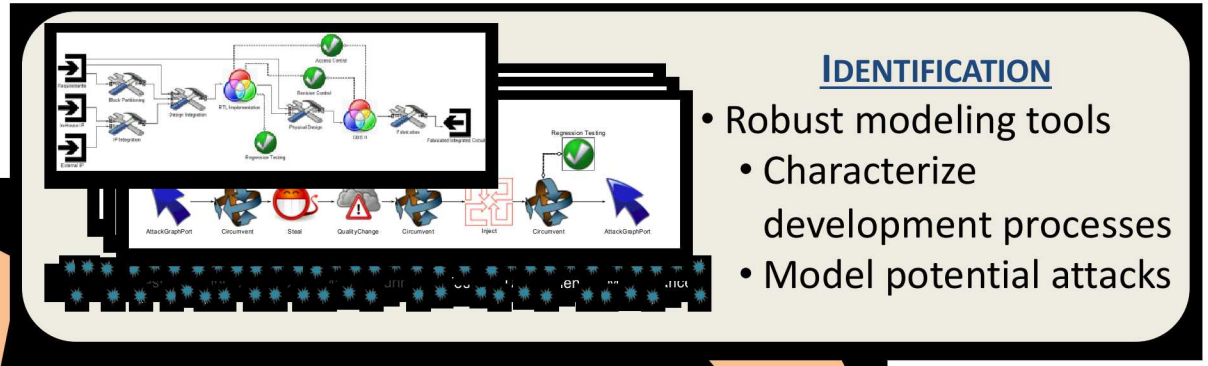
The Challenge: Protecting the Unknown

- Supply Chain networks are large, deep, and complex, spanning the globe
  - Challenging to completely map
    - Distance aspects of the supply chain may be opaque to system developers
  - Extremely challenging to completely isolate
- Adversaries attempt to undermine development processes and supply chains
  - Adversary model: **intelligent, highly motivated, well-funded, very creative**
    - Diverse goals: disruption, subversion, counterfeit, integrity violation
  - System developers cannot know with certainty:
    - Who, where, when, or how adversaries may impact a system
- Problem:
  - We **must develop and deliver systems** that work as expected
  - We **cannot isolate** ourselves from the adversary
  - We **cannot predict with certainty** adversarial actions
  - ***How do we protect our systems from subversive manipulation*?**



PRESTIGE: PRactical Evaluation and Synthesis of Trust In Government systEms

- Research effort at Sandia National Laboratories to quantitatively evaluate risk of development-time manipulation
- Rigorous visual modeling to capture both supply chains/development processes and attack graphs targeting system development
- Utilize game theory to evaluate dynamics of interaction between attacker and defender to understand risk

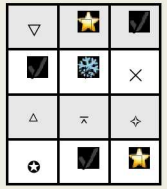


IDENTIFICATION

- Robust modeling tools
  - Characterize development processes
  - Model potential attacks

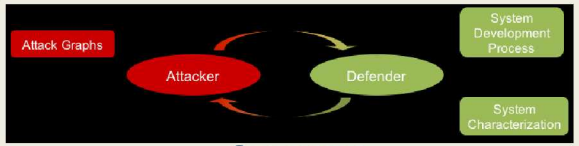
TRADEOFF ANALYSIS

- Constraints driven risk mitigation analysis
- Mathematical characterization of mitigation impact



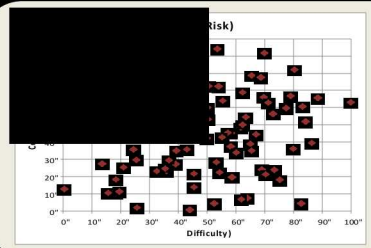
EXEMPLAR

SPACE SYSTEMS



ANALYSIS

- Game theory-based risk analysis
- Tractable attack evaluation



INFERENCE

- Optimization-guided exposure of highest areas of risk