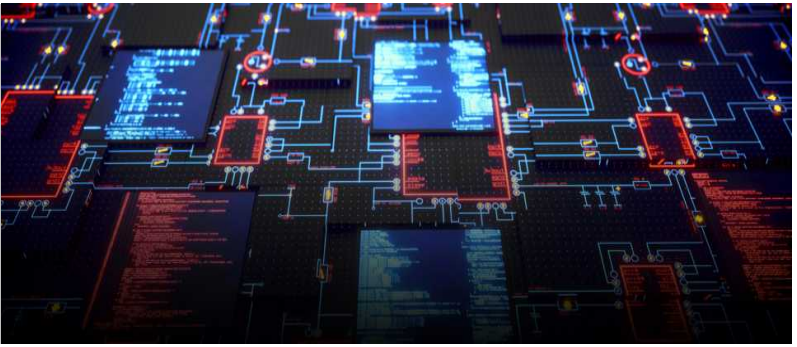
SAND2018-0974PE



Assessment Foundations for DARPA's CASE

Katie Sutton
Manager, Cyber Systems Security R&D
kesutto@sandia.gov
(505)-845-9717

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.

Assessment Foundations for DARPA CASE

- Sandia conducts security assessments of a wide range of systems and components
  - Nuclear Weapons
  - Enterprise networks
  - Non-traditional systems: cyber-physical (ICS, IOT, PPS), military platforms, etc.
- Assessments require careful planning and execution to realize their potential to provide significant return on investment
- A strategy is needed to assess CASE developer products to maximize impact and provide early opportunities for improvement

Assessment Strategy

- Key considerations:
  - What questions do the assessments need to answer – are they same for the different program phases, technical areas, performers, etc.?
  - How will the program manager use the results, e.g., go/no-go decisions, use discretionary funds, determine course of action?
  - How will the developers use the results, e.g., prioritize next steps, mitigate weaknesses?
- Subject Matter Experts need to be matched to the specific assessment
  - Are different SMEs needed for different products or to answer different questions?
    - E.g., how and to what extent is the system resilient? Are there attack vectors software hardened through formal methods does not mitigate?
- What is in scope and what is out?
- Can the developer re-run earlier tests after mitigations have been applied, before end of next phase testing?

Assessment Strategy

Sandia National Laboratories

- Early assessments performed in cooperation with the developers should be especially productive
  - A design assurance mentality guides us to identify as many security flaws as possible so they can be fixed early
- Each assessment should start with the end in mind, then the assessment can be tailored to meet program phase objectives
  - Measures of Performance & Metrics: program requirements, developer assertions, resilience definition, confidentiality, integrity, and availability, etc.
  - Risk Management: what are the risk scenarios (e.g., attack graph), what are the consequences, and how hard or easy is it for different adversaries to defeat the developer products?
- Final phase assessments should demonstrate achievement of requirements, and mitigation against attacks identified in earlier phases

Formal Approach to Attacking Formally Verified Systems

Sandia National Laboratories

- FV provides rigorous guarantees on a digital model (great for security), but...
- Did the FV analysis verify the *right properties*?
  - May be impractical for developers to formalize & prove *all* requirements
  - Red team can perform its own FV on properties not covered by developers to seek counterexamples (i.e., vulnerabilities)
- Did the FV model capture the *right semantics*?
  - Probe the "seams" to exploit behaviors that weren't considered in the FV
    - If C code was verified, could the compiled object code still be vulnerable?
    - Could analog physical phenomena alter semantics assumed by developers?
  - Can expose new vulnerability modes and guide other red-team activities such as fuzzing

Cyber Resilience Capability Foundations

- Cyber resilience provides risk management perspective to complemen cyber security efforts
- Cyber resilience capabilities integrate cyber security expertise with a multi-disciplinary, science-based foundation
  - Mathematics (control & network theory, optimization)
  - Data analytics
  - Adversary modeling

- Strong foundations and experience provide confidence in assessments and recommendations

Theory + Modeling + Validation → Provably Resilient Systems

Assessment Foundations - Summary

Sandia National Laboratories

- In order for assessments of developer products to be useful, a strategy is needed
- SMEs need to be matched to specific assessments
- Early assessments performed in cooperation with the developers should be especially productive
- Each assessment should start with the end in mind, then the assessment can be tailored to meet program phase objectives
- A strategy shared between the PM, the developers, and the assessors will maximize the ROI

Sandia National Laboratories

Questions?

Also see:

http://idart.sandia.gov

Katie Sutton
Manager, Cyber Systems Security R&D
kesutto@sandia.gov
(505)-845-9717