SAND2018-1498PE

February
2018

Assessment Foundations for DARPA's CASE

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

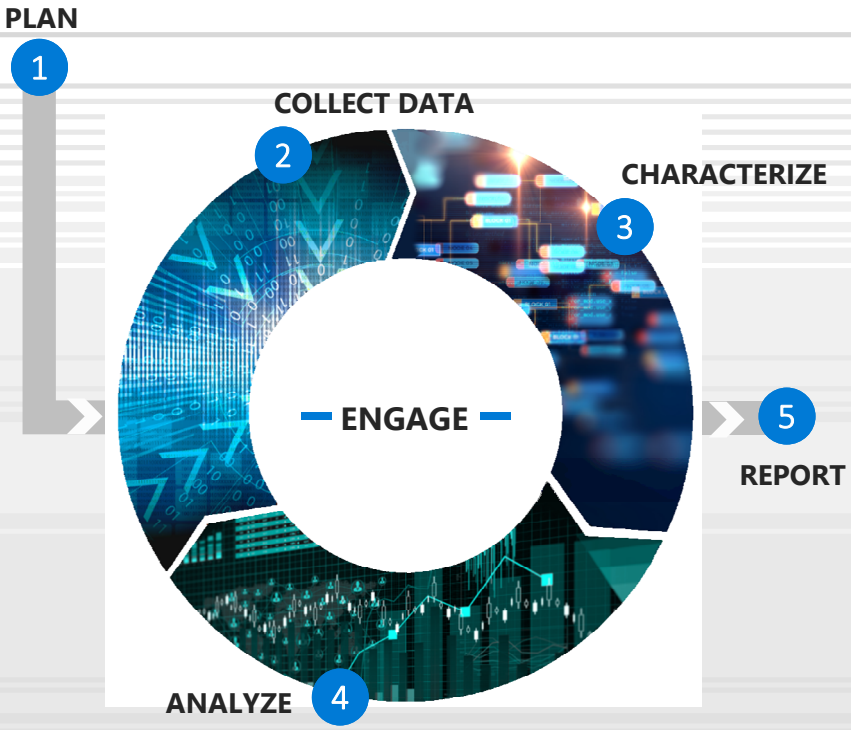
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract.

CYBER RESILIENCE CAPABILITY FOUNDATIONS

- Cyber resilience provides risk management perspective to complement 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



- 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

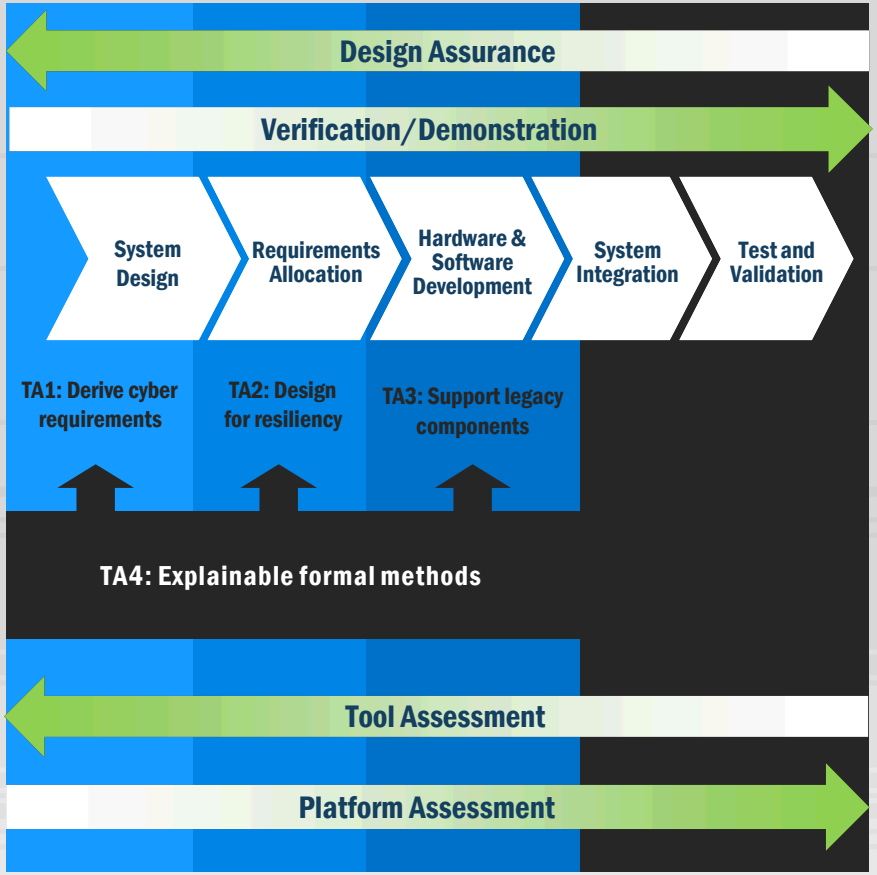
- Key considerations:
  - What questions do the assessments need to answer – are they same for the different program phases, technical areas, performers, etc.?
  - How will the program manager use the results, e.g., go/no-go decisions, determine course of action?
  - How will the developers use the results,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

RESILIENCE CONSIDERATIONS

	Vulnerability Assessment	Resilience Assessment
Focus	Find and mitigate vulnerabilities	Evaluate and improve ability to cope with exploited vulnerability (known or unknown)
Assumptions	Security is enhanced by addressing identified vulnerabilities	Resilience enables system to continue core functionality and rapidly recover after adversary is in system
Metrics	Generally focus on CIA (confidentiality, integrity, availability)	Generally focus on impact to mission: magnitude, duration, and resource usage

Resilience assessments often leverage common system information but provide an alternative set of insights and recommendations.

ASSESSMENT STRATEGY



- Early assessments performed in cooperation with the developers can be especially productive
- 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 demonstrate achievement of requirements, and mitigation against attacks identified in earlier phases

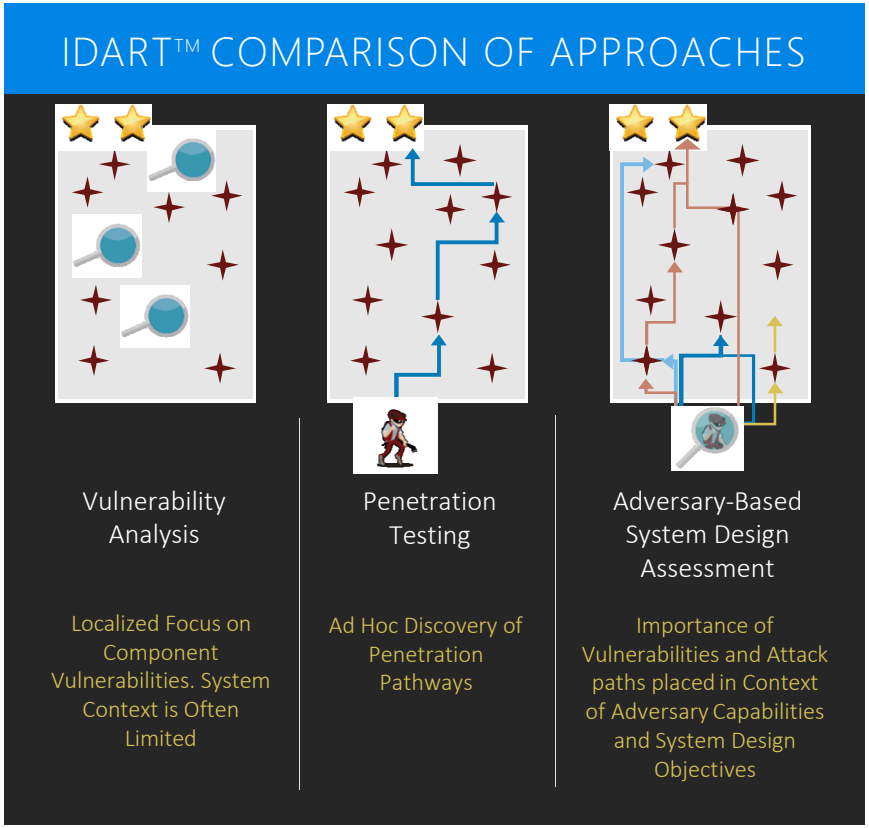
Assessment evolve throughout the process and build upon earlier phases

FORMAL APPROACH TO ATTACKING FORMALLY VERIFIED SYSTEMS

- 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

ASSESSMENT FOUNDATIONS - SUMMARY

- In order for assessments of developer products to be useful, a strategy is needed
- SMEs need to be matched to specific assessments
- Each assessment should start with the end in mind, then the assessment can be tailored to meet program phase objectives
- Resilience assessments can be highly complementary to traditional vulnerability assessments and provide additional insights
- A strategy shared between the PM, the developers, and the assessors will maximize the ROI

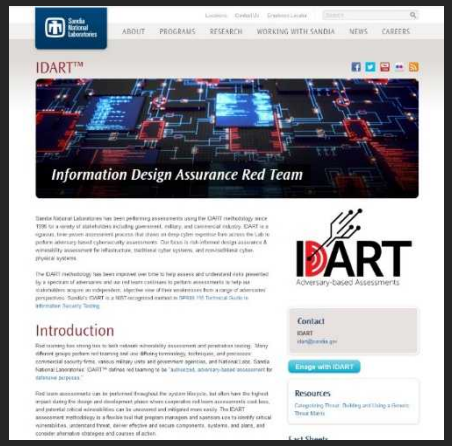


QUESTIONS?

Katie Sutton

Manager, Cyber Systems Security R&D

kesutto@sandia.gov | (505)-845-9717



Also see:
idart.sandia.gov