Configuration Security (ConSec)

Mr. Jacob I. Torrey

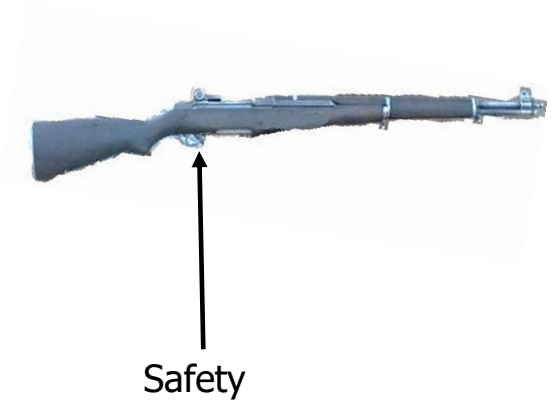
Proposers Day

November 17, 2017

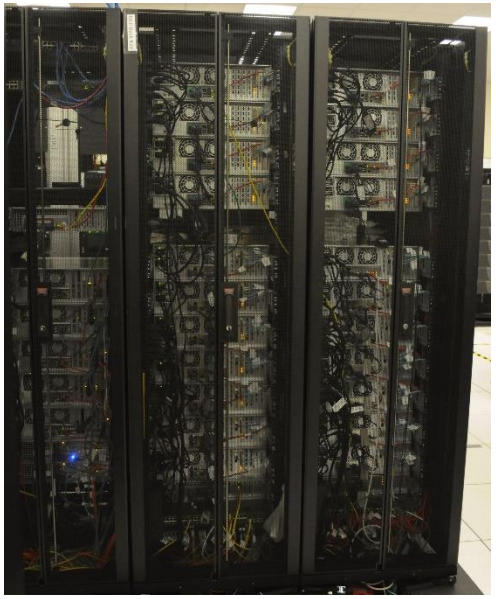
ConSec objective statement

Develop a system to automatically generate, deploy, and enforce secure configurations of components and subsystems for use in military platforms

Configuration complexity is a major source of vulnerabilities



M1 Garand



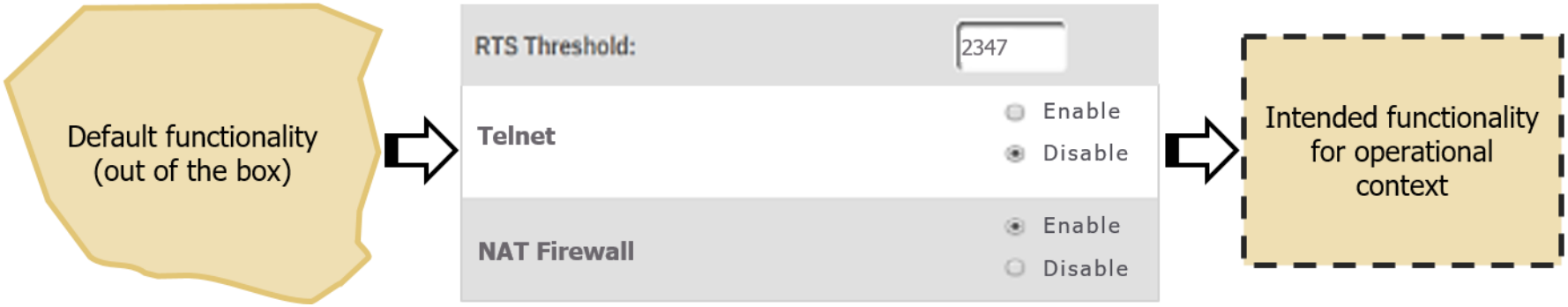
Partial representation of weapons platform network

Source: https://www.flickr.com/photos/145317968@N02/32207891206/

Source: https://www.flickr.com/photos/dcoetzee/6271688256/

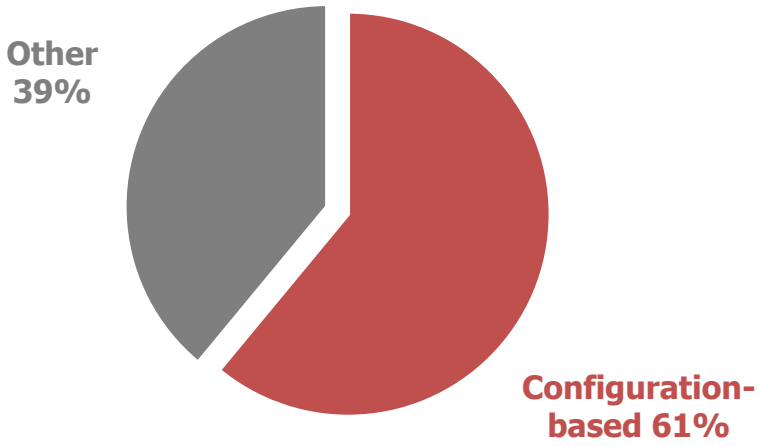
Configuration complexity is a major source of vulnerabilities

Example configuration settings



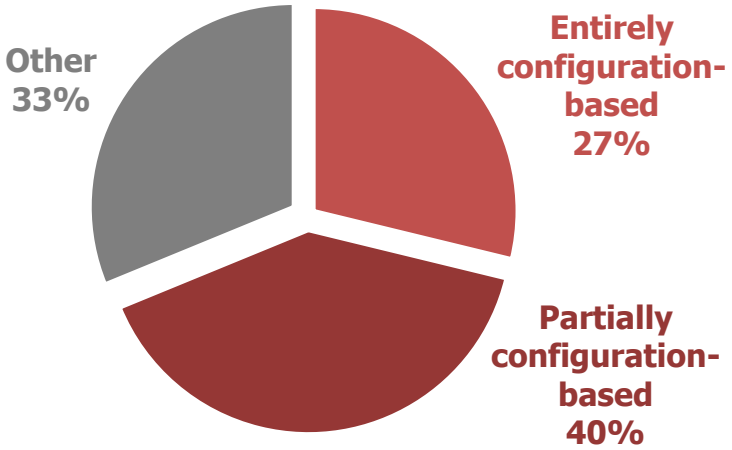
Source: Screenshot of Verizon home router

Failure scenarios of power grid



Electric Power Research Institute classification of power grid failure scenarios

Real-world IT penetration-test findings



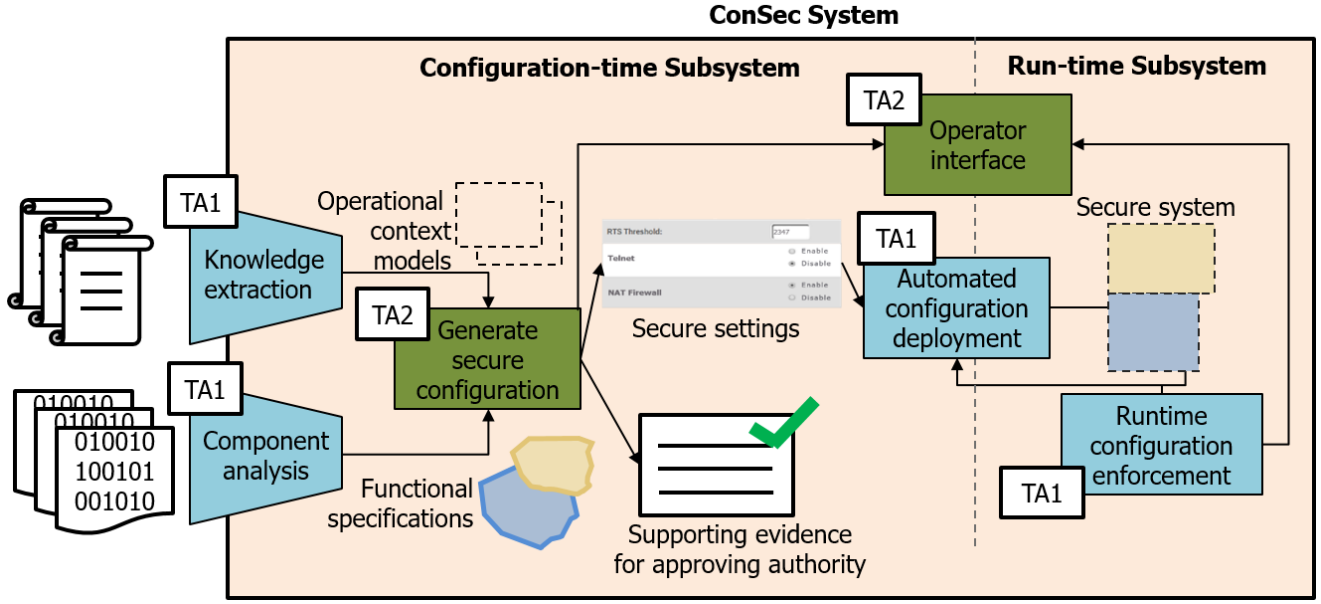
Cobalt.io pen-test metrics report of 1500 vulnerability findings, 2016

ConSec vision

- Develop a system to
  - Explore configuration state space, deploy secured settings, and monitor for deviation

TA1: Understand composed system
- Build model of functionality and operational contexts

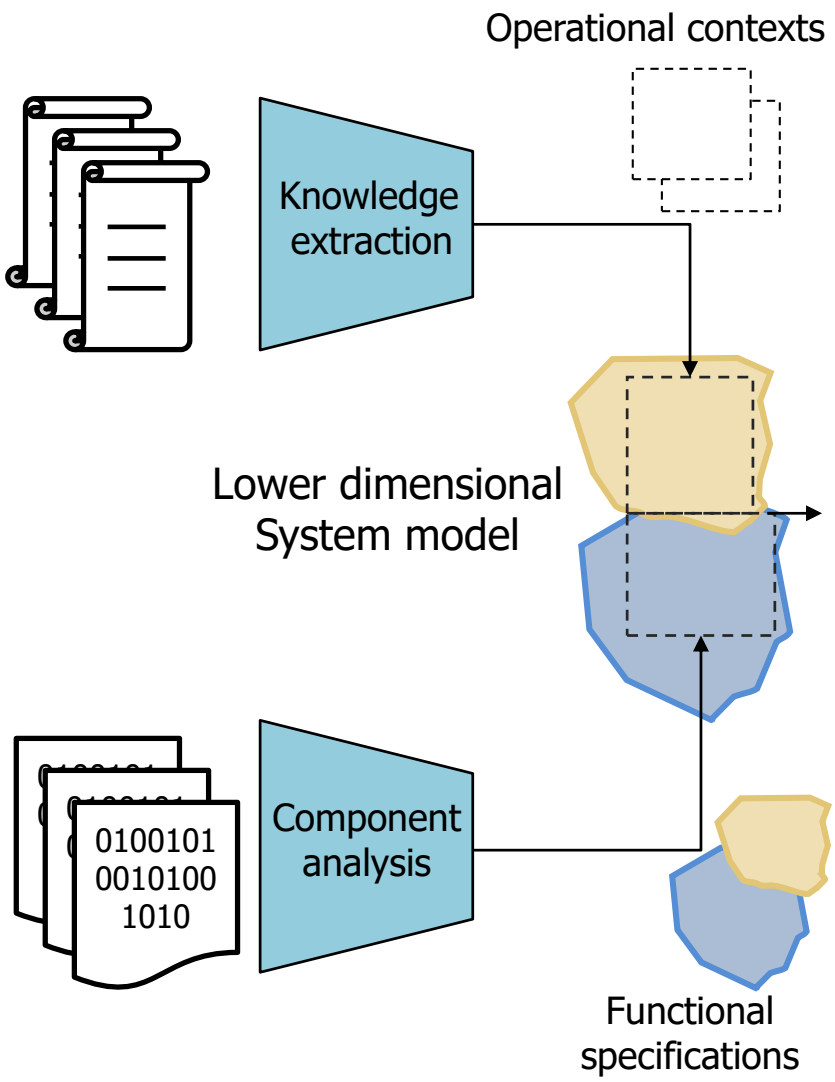
TA2: Generate secure configuration optimized for operational contexts



- TA3: Voice of the offense
  - Challenge TA1/TA2 system with configuration and composition vulnerabilities
- TA4: Evaluation and integration
  - Target platform provider and integrator

TA1: Understand composed system

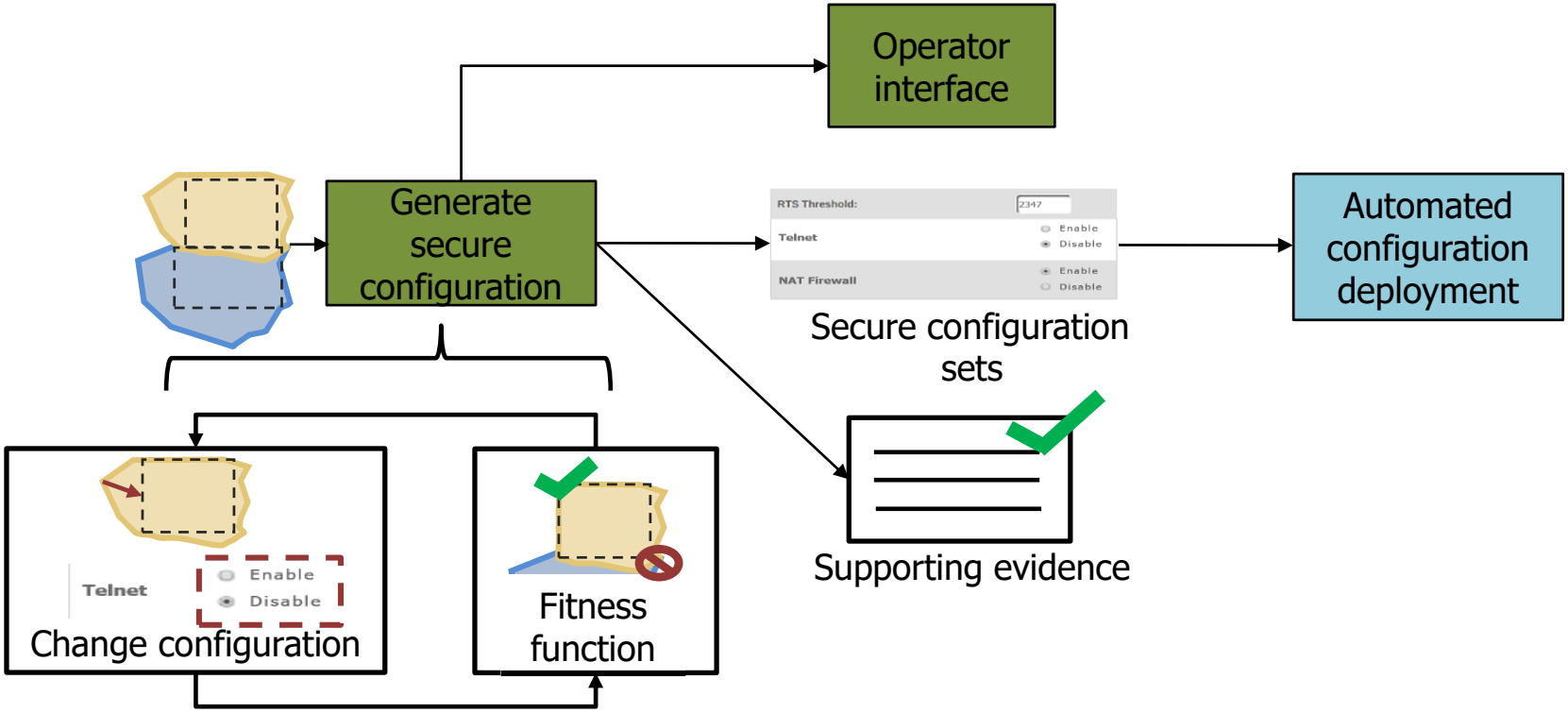
- Represent the operational context of a composed system in a model
- Rapid ingest of human-readable system documentation
- Automated generation of configuration-aware functional specifications
- Reducing dimensionality of configuration parameters
- Deployment and monitoring of configuration sets on target system



TA1 challenges

- Semantic extraction to produce a model of configuration parameter functionality relative to system behavior
- Principled reduction of the configuration space for each component
- Semi-automated modeling of operational context(s) of the target system from human-readable documentation
- Automatically generate a specification of each component's functionality based on its software, firmware and configuration parameters
- Develop a vendor-agnostic representation for communicating these models and specifications to the TA2 system
- Develop a capability to access and modify the configuration parameters on diverse devices

TA2: Generate secure configuration



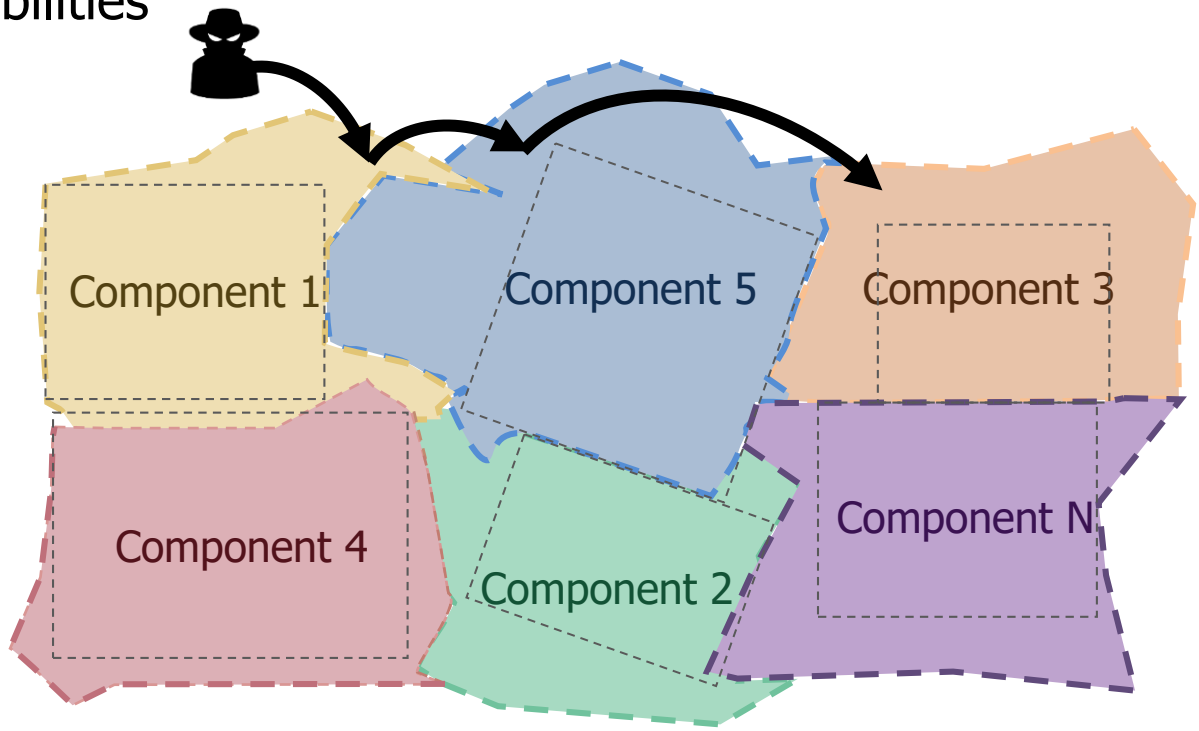
- Rapidly generate mission-optimized configurations
- Support authority-to-operate approval of configuration sets with formalized arguments
- Enable large scale context-sensitive reasoning with incomplete specifications
- Discover hidden behaviors in composed systems

TA2 challenges

- Performing compositional analysis of the TA1-provided system models and specifications to determine an optimal configuration set for the target in each operational context
- Automatically generating human-readable evidence supporting the selected configuration set in order to allow authorization approval
- Communicating the configuration state of the system with the TA1-developed monitoring subsystem to detect indicators of compromise or assist in changing between operational contexts

TA3: Voice of the offense

- Challenge TA1/TA2 system with configuration and composition vulnerabilities



- TA3 proposals should address the following challenges
  - Develop tools, techniques, and procedures to exploit composed systems solely via configuration- or composition-enabled vulnerabilities
  - Use TA1-provided models and specifications to guide the generate of attack paths, minimizing human-in-the-loop effort

TA4: Evaluation and integration

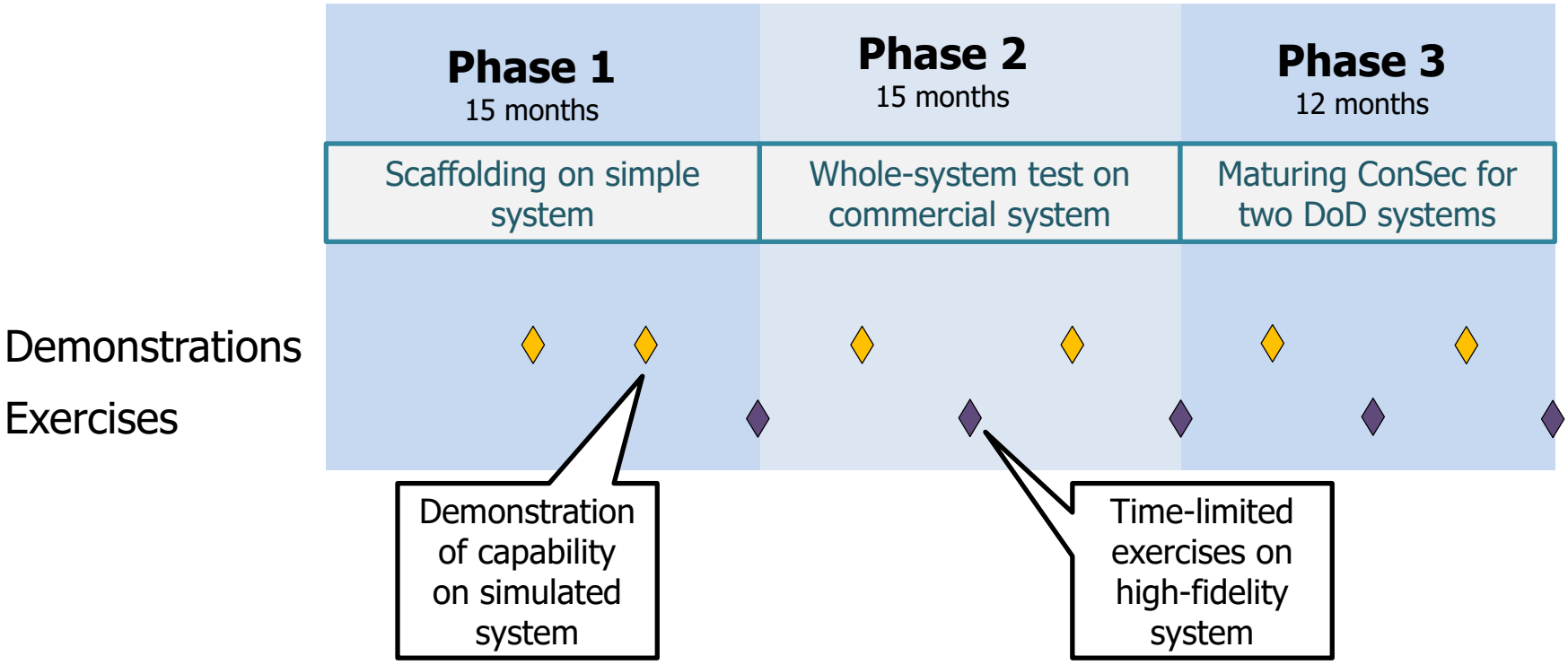
- Technical progress assessment
  - Conduct functional, regression, performance, and scalability testing
  - Provide specific, constructive feedback to all performers developing code
- Evaluations
  - Develop relevant test cases for integrated TA1/TA2 systems and measure performance against system-specific metrics
  - Conduct evaluations in advance of PI meetings to inform the technical discussion
- Exercises
  - Plan, develop and coordinate program exercises
  - Exercises will increase in complexity and duration over the period of performance

- TA4 proposals should address the following challenges
  - Facilitation of common data formats between TA1 and TA2
  - Coordination of exercises on limited physical target systems
  - Metrics evaluation and novel metrics to measure the progress and success of the ConSec system

ConSec program metrics

	Phase 1 (scaffolding)	**Phase 2** (initial deployment)	**Phase 3** (Highly-complex system)
TA1: Model Fidelity	80% of static space	80% of static space	90% of static
TA1: Documentation Ingest	10x manual, 60% accuracy	10x manual, 70% accuracy	10x manual, 80% accuracy
TA1: Deployment time	1.5x faster than manual	5x faster than manual	15x faster than manual
TA2: Configuration-space coverage	60% coverage	60% coverage	75% coverage
TA2: Risk reduction	85% reduction	85% reduction	85% reduction
TA2: Correctness guarantee	None	Basic	Formal

ConSec schedule



Program funding

- Total program funding available for award is $45m over 3 1/2 years
- Proposals may address only one Technical Area
- Organizations can submit proposals to all Technical Areas
  - Which to consider for award is at the discretion of the Government
  - TA-4 performer may perform on other TAs subject to an acceptable OCI Mitigation Plan

To summarize

- Read the BAA, carefully and more than once
  - *"Specifically excluded is research that primarily results in evolutionary improvements…"*
  - DARPA does not acquire commercial products

- The goal of ConSec is to automatically generate, deploy, and enforce secure configurations of embedded COTS/GOTS devices for use in military platforms

www.darpa.mil