Statistical Test Optimization for Cyber Test

Mary Kim, Peter Kraus, Neal Mackertich, Tonja Rogers

Date: March 8, 2018

Raytheon CODE Center
CYBER OPERATIONS
DEVELOPMENT & EVALUATION

Approved for Public Release
Copyright © 2016 Raytheon Company. All Rights Reserved.
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Raytheon's Cyber Vision and Objectives

Vision

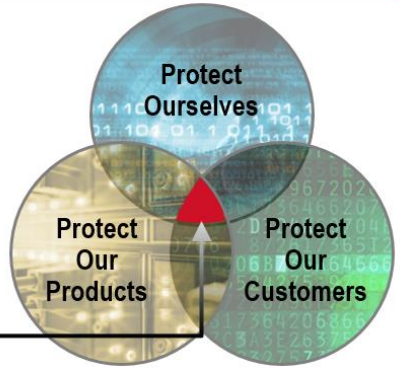
Be the best at:

- Protecting our internal systems
- Protecting our customer products
- Protecting our customers by providing timely Cyber capabilities

World-Class Capabilities

- Threat Understanding
- End-to-End Capabilities
- Testing and Verification
- Cyber Domain Knowledge
- Real Use of Products
- Scalability of Products
- Hardening of Systems

Objectives



CODE Center is a key enabler of RTN's Cyber Strategy

The Raytheon Cyber Operations, Development and Evaluation (CODE) Center is a state-of-the-art cyber range available for internal customer work to test and ensure the resiliency of existing and future mission-critical systems against cyberattacks.

Raytheon CODE Center
CYBER OPERATIONS
DEVELOPMENT & EVALUATION

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Introduction

- Statistical Test Optimization (STO) is a proven industry best practice approach used to improve both test coverage and test case efficiency
- After presenting and discussing the general case, this presentation discusses the use of these same statistical methods for Cyber Security Testing
  - Why do this?
    - Increase in the need for cyber testing
    - Shortage of cyber security test SMEs
    - Need increased return on test dollars spent
      - More test coverage for less money
- Our Goal – Demonstrate ability to improve coverage of cyber test and increase repeatability through the use of STO

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Agenda

- Overview of Statistical Test Optimization (STO)
  - What is STO?
  - Example of application of STO
- Applying STO methods to Cyber Security Testing
  - Our focus areas
    - Penetration Testing
    - Fuzz Testing
- Conclusion

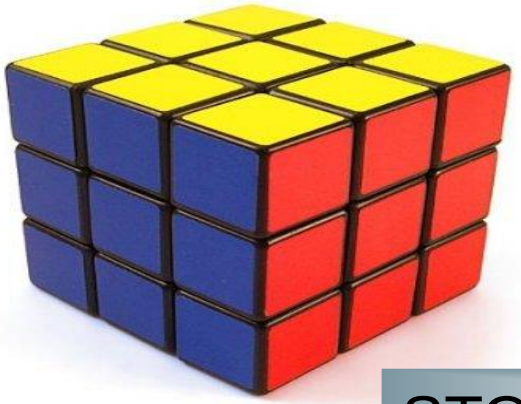
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

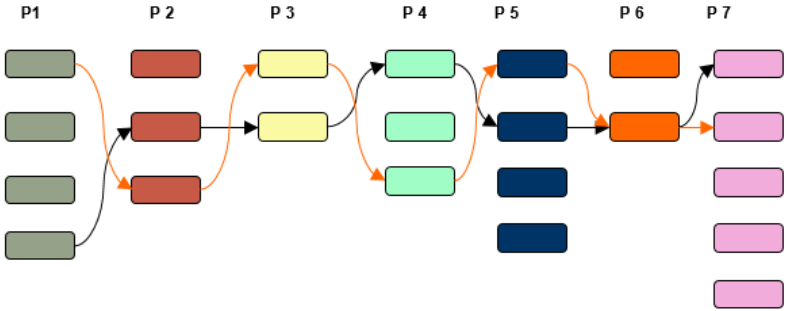
Statistically-Based Test Optimization

Raytheon

Testing all possible combinations is typically infeasible!

- **When you must test a subset of all combinations– how to choose an appropriate subset?**
- **The integrated application of statistical methods, most notably Design of Experiments (DOE) & Combinatorial Design Methods (CDM), has been cited by the Department of Defense as an industry best practice in this space.**





All possible Test cases = 2880 tests

STO = Domain Knowledge + Mathematics

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Electronic Warfare Case Study
Original vs Alternate Test Plan Coverage Analysis

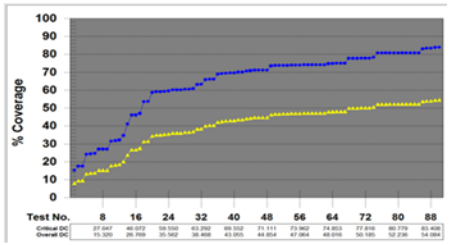
Raytheon

Original Traditional Test Plan:

90 Test Cases

Coverage Analysis Tool results

- 2-Ways: 67.9%
- 3-Ways: 35.2%
- 4-Ways: 15.5%
- Missing 2-Ways: 144 (168 Total – 24 Constraints)

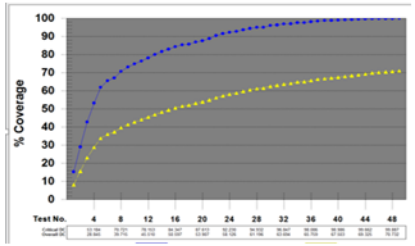


STO Generated Test Plan:

49 Test Cases (45% reduction)

Coverage Analysis Tool results

- 2-Ways: 100%
- 3-Ways: 61.3%
- 4-Ways: 23%
- Missing 2-Ways: 0



Generally see a 20-30% improvement when using STO

Approved for Public Release

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Electronic Warfare Case Study
Combinatorial Test Constraints

Raytheon

Factors and Levels:

	Platform Type	Frequency	Frequency Type	PRI	PRI Type	PW	Scan	Scan Type
Level 1	Missile	Band 1	Constant	CW	CW	CW	None	Steady
Level 2	Aircraft	Band 2	Agile	Very Low	Constant	Narrow	Fast	Circular
Level 3	Ship	Band 3 Low		Low	Switcher	Medium	Medium	Conical
Level 4	Land	Band 3 High		Medium	Jitter	Wide	Slow	Sector
Level 5		Band 4		High	Stagger			

64,000 total possibilities without Constraints

CW-related constraints

- PRI [CW] with PRI Type [Constant, Switcher, Jitter, or Stagger]
- PRI Type [CW] with PRI [Very Low, Low, Medium, or High]
- PW [CW] with PRI Type [Constant, Switcher, Jitter, or Stagger]
- PW [CW] with PRI [Very Low, Low, Medium, or High]

Scan-related constraints

- Scan [None] with Scan Type [Circular, Conical or Sector]
- Scan Type [Steady] with Scan [Fast, Medium, or Slow]

Constraints:

	If Factor ...	is at level ...	then Factor ...	can't be ...
Constraint 1	PW	CW	PRI Type	Constant
Constraint 2	PRI	CW	PRI Type	Switcher
Constraint 3	PRI	CW	PRI Type	Jitter
Constraint 4	PRI	CW	PRI Type	Stagger
Constraint 5	PRI Type	CW	PRI	Very Low
Constraint 6	PRI Type	CW	PRI	Low
Constraint 7	PRI Type	CW	PRI	Medium
Constraint 8	PRI Type	CW	PRI	High
Constraint 9	PW	CW	PRI Type	Constant
Constraint 10	PW	CW	PRI Type	Switcher
Constraint 11	PW	CW	PRI Type	Jitter
Constraint 12	PW	CW	PRI Type	Stagger
Constraint 13	PW	CW	PRI	Very Low
Constraint 14	PW	CW	PRI	Low
Constraint 15	PW	CW	PRI	Medium
Constraint 16	PW	CW	PRI	High
Constraint 17	Scan	None	Scan Type	Circular
Constraint 18	Scan	None	Scan Type	Conical
Constraint 19	Scan	None	Scan Type	Sector
Constraint 20	Scan Type	Steady	Scan	Fast
Constraint 21	Scan Type	Steady	Scan	Medium
Constraint 22	Scan Type	Steady	Scan	Slow

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Leading Change & Driving for Business Results

"There is no way around it - we have to find ways to do more with less. The integrated program use of statistical techniques such as Design of Experiments, have proven themselves to be powerful enablers in our test optimization efforts to reduce cost and cycle time while providing our customers with confidence that our systems will perform."

Dr. Tom Kennedy

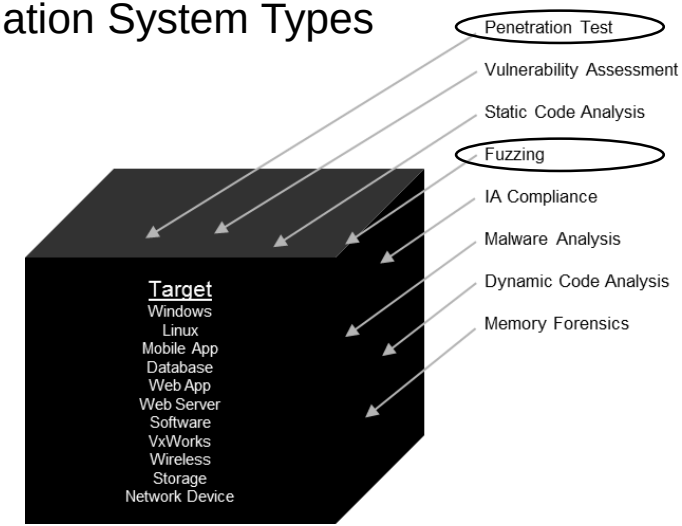
Chief Executive Officer

Raytheon Company

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Cyber Test

- Cyber Test is focused on a broad area
  - Test Methods
  - Information System Types



- Where best to apply STO?

- Experimented with applying STO techniques a couple of areas

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Penetration Testing

Raytheon

- Traditional approach
  - Using information obtained through the use of software applications or manual procedures to identify possible entry points into a network or actually breaking into a network
  - Requires a senior cyber SME with very broad knowledge to be successful

- Statistical Test Optimization (STO) approach
  - Utilize STO to generate a standard test suite and plan that can be filtered based upon the system under test to produce consistent and repeatable testing parameters
    - Enables a more junior cyber tester to be more thorough and effective
    - Ensures the same type of testing is performed on every system
      - Allows repeatability, ability to develop test cost models, and provides a job aid for testers

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

PEN test example

- Creating a Test Plan that provides guidance on common vulnerabilities to test against a specific system configuration

Factors and Levels

	Factor 1	Factor 2	Factor 3
Factor Name:	**Port**	**OS**	**IS Type**
Level 1	21	Linux	network
Level 2	22	Windows	storage
Level 3	23		server
Level 4	25		
Level 5	80		

With Constraints

	If Factor ...	is at level ...	then Factor ...	can't be ...
Constraint 1	Port	25	IS Type	network
Constraint 2	Port	25	IS Type	storage
Constraint 3	IS Type	network	OS	Windows
Constraint 4	IS Type	storage	OS	Windows

Produces 14 Optimized Test Configurations

	Factor_A	Factor_B	Factor_C
Factor Name	Port	OS	IS Type
Case 1	25	Windows	server
Case 2	21	Linux	storage
Case 3	22	Linux	storage
Case 4	80	Windows	server
Case 5	21	Windows	server
Case 6	23	Windows	server
Case 7	80	Linux	network
Case 8	23	Linux	storage
Case 9	21	Linux	network
Case 10	22	Windows	server
Case 11	22	Linux	network
Case 12	23	Linux	network
Case 13	25	Linux	server
Case 14	80	Linux	storage

31 Total Possible 2-way Combinations (before constraints)

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Cyber Vulnerability Test Cases

Raytheon

Apply known vulnerability test

To applicable Test Configurations

	Port	OS	IS Type	Weak Password	No Access Control	Insufficient Access Control	Blank Password	Anonymous FTP Access Allowed(Write Access)	Anonymous FTP Access Allowed(Read Access)	Weak Warning Banner	Missing Warning Banner	Missing or Outdated Patches	Mail Relaying Allowed	Mail Spoofing Allowed	Default Credentials Found	Unnecesssary TCP Services are Open	Excessive File and Directory Permissions Granted to General Users	No Access Control on Remote Protocols	Cleartext Protocol
Vuln_Name																			
Case 1	25	Windows	Server																
Case 2	21	Linux	Storage																
Case 3	22	Linux	Storage																
Case 4	80	Windows	Server																
Case 5	21	Windows	Server																
Case 6	23	Windows	Server																
Case 7	80	Linux	network																
Case 8	23	Linux	Storage																
Case 9	21	Linux	network																
Case 10	22	Windows	Server																
Case 11	22	Linux	network																
Case 12	23	Linux	network																
Case 13	25	Linux	Server																
Case 14	80	Linux	Storage																

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Fuzz Testing

- Traditional approach
  - Input massive amounts of random data to flood, and overwhelm a system in hopes of identifying bugs and vulnerabilities
    - Can takes a very long time to uncover an issue
- Statistical Test Optimization (STO) approach
  - Use STO to at least ensure you are providing a set of ‘randomness’ that is evenly distributed by statistically varying parameter inputs in a mathematically defined way (using orthogonal arrays) enabling improved coverage of test space parameter interfaces
  - Additionally use your knowledge of the system under test to focus in on very specific parts / specific weaknesses of the system through the integrated use of parameter and parameter weighting techniques

Approved for Public Release
This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Conclusion

- STO can be a valuable tool in the area of Cyber Test!
  - Demonstrated a reduction in overall number of Test Cases while ensuring test coverage of critical test parameters and their interfaces
- Next Steps
  - Continue to expand on Pen Test information in order to develop comprehensive test plans that can be repeatable
  - Continue to evaluate applying STO to Fuzz Test in order to get the same results with minimum amount of test

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

BIOs

Mary Kim, CISSP-ISSEP, CEH, GREM

Mary Kim works as a Senior Principal Cyber Security Engineer for Raytheon Company. She graduated with a Bachelors in Electrical Engineering and a Masters in Computer Information Systems. Mary has been working in the Cyber and Information Assurance (IA) realm for 20 years. In addition to providing Cyber and IA support to both commercial and government programs, Ms. Kim also works as an instructor/mentor teaching Cyber Security courses. Areas of focus include penetration testing, vulnerability assessment, IA Compliance, Malware Analysis, and Risk Management Framework.

Dr. Peter Kraus is an Engineering Fellow focusing on statistical engineering training and consulting efforts within Raytheon Integrated Defense Systems. Peter is responsible for implementing Design for Six Sigma techniques across Engineering and Operations to achieve Mission Assassurance. Peter earned a Masters Degree in Mathematics from Northeastern University and a Ph.D. in Operations Research from UMass Amherst.

Dr. Neal Mackertich is an Engineering Fellow within the IDS Engineering Systems Architecture, Design & Integration Directorate (SADID). During his 25+ years at Raytheon, Neal has held positions of increasing responsibility within both Engineering and Program Management including that of Systems IV&V Lead and Director of the Raytheon Six Sigma Institute. Neal is presently responsible for Systems Engineering enablement of Mission Assurance through product & process performance modeling & optimization. Neal holds a BS in Chemical Engineering, a MS in Engineering Management and Ph.D. in Engineering Operations Research from the University of Massachusetts-Amherst.

Tonja Rogers is an Engineering Fellow at Raytheon's Cyber Operational Development and Evaluation (CODE) Center based in Dulles, VA. During her 35+ years at Raytheon, Tonja has held various positions within Engineering focused on System Level Integration and Test of large air defense systems. She has spent the past two years applying those methodologies to cyber test as a Cyber Test Lead. Applying Statistical Test Optimization (STO) to test is an area that Tonja has focused on over the years, and is excited to explore in the area of cyber. Tonja holds a BS in Electrical Engineering, and a MS in Electrical Engineering focused on Electromagnetics from New Mexico State University.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.