FloCon 2020

Using Data to Defend

JANUARY 6–9, 2020 | SAVANNAH, GEORGIA

Methods for Testing and Qualifying Analytics

Timothy Shimeall, Ph.D.

CERT Situational Awareness Group

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

FloCon 2020

Using Data to Defend

JANUARY 6–9, 2020 | SAVANNAH, GEORGIA

Methods for Testing and Qualifying Analytics

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1255

Overview

Motivation and Definitions

Example Analytic

Test Framework

Qualifying Analytics

Motivation

It’s only an analytic
- Just run it and see if it works
- It’s only needed for this one incident
- It’s too simple to worry about

I’m an analyst
- Not a developer
- Not a test/QA person
- Too busy for test

Takes too long to build (or fix)

Code starts generating poor results
- False positives / false negatives
- Too many resources needed
- Bugs / crashes / odd messages

Next person has to deal with it
- Poor idea what it does
- No clear flow of logic
- Mix of scripts/structures/languages

Definitions

Analytic: A particular process that examines data to find trends and answer questions

- Descriptive analytics: find range and central tendency statistics on traffic
- Diagnostic analytics: track indicator that flags data exfiltration
- Predictive analytics: track indicator that suggests scanning prior to compromise
- Prescriptive analytics: flag traffic that is banned by policy

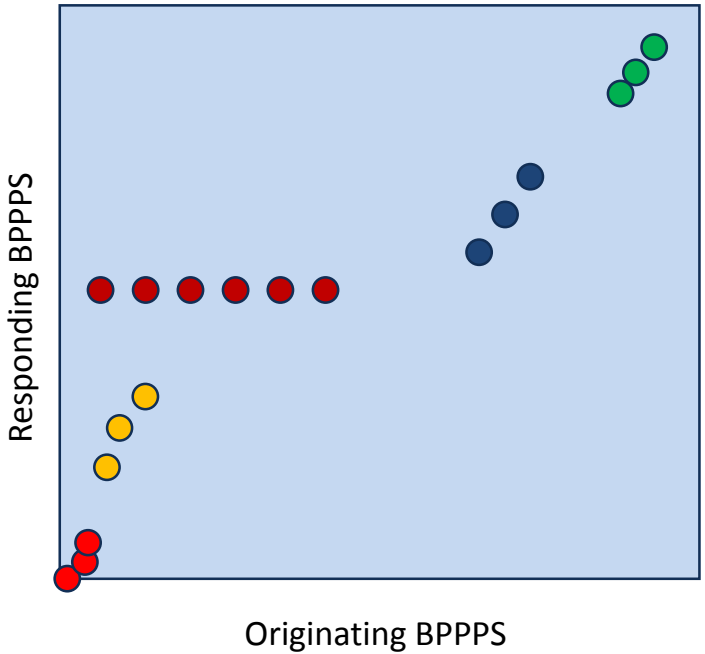
https://www.mastersindatascience.org/resources/what-is-data-analytics/

Test: A procedure intended to establish the quality, performance, or reliability of something, especially before it is taken into widespread use.

Qualify: Be entitled to a particular benefit or privilege by fulfilling a necessary condition.

https://www.lexico.com/en/definition/test

BPPPS Analytic



Flow bytes per packet per second analytic

Mixing volumes and timing to separate:

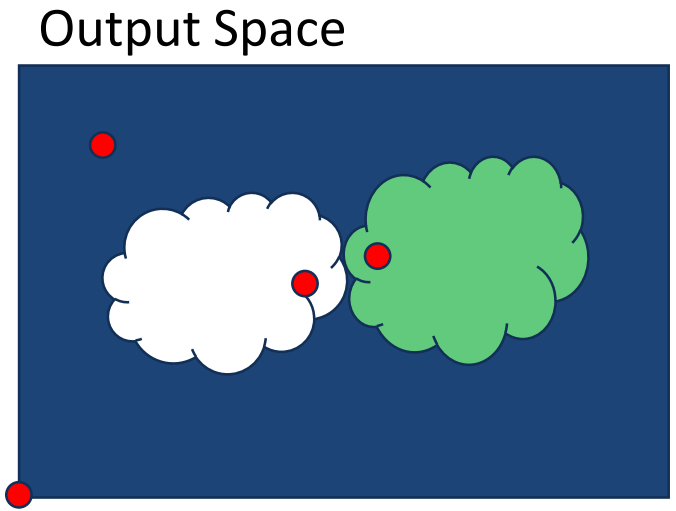
- Signaling overhead (redundant close)
- Common attacks (brute force, port knocking)
- File transfer
- Interactive traffic

Port agnostic, not signature-based

Test Design -1

Data driven testing

- Normal input
- Null input
- Input for each output

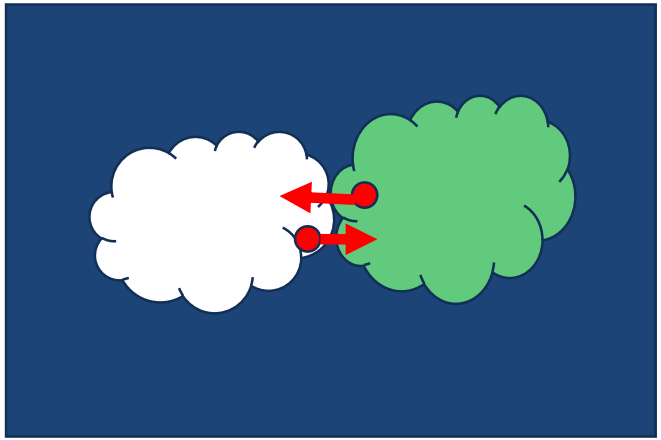


Test Design - 2

Case driven testing

- Where small addition changes output
- Where small deletion changes output
- Where reordering changes output

Output Space

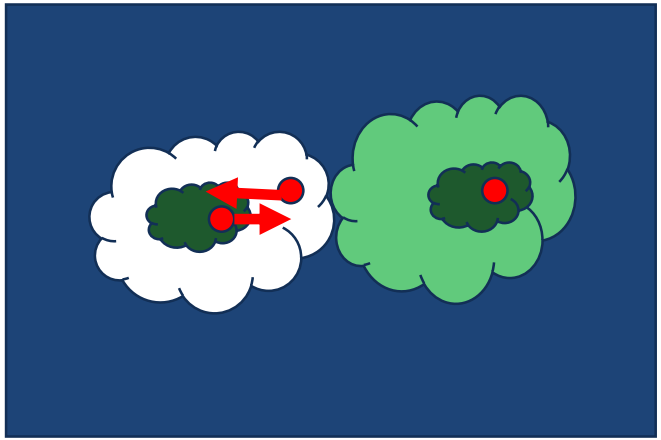


Test Design – 3

Threat Driven:

- Sample outputs associated with threats
- Where small addition can move non-threat to threat
- Where small deletion can move threat to non-threat

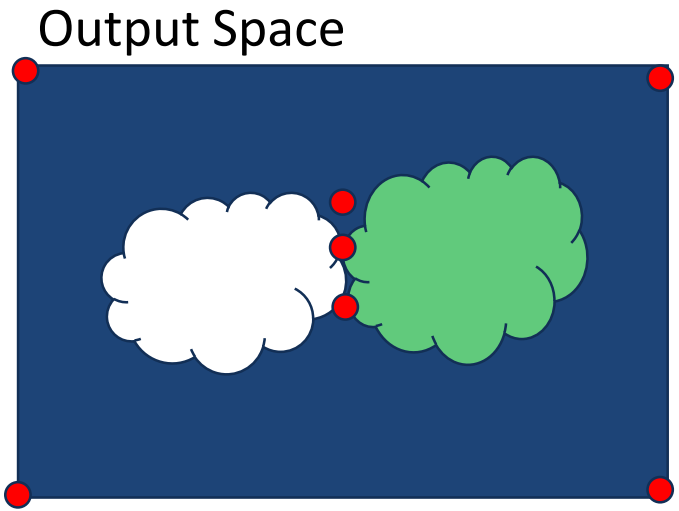
Output Space



Test Design - 4

Bug-driven

- Where most likely omissions
- Where most likely confusions
- Where potential incompatibilities



Qualifying Analytics

Reliability

Trust

Robustness

Maintainability

Compatibility

Security