



Analytical Evaluation Framework

Tim Shimeall
CERT/NetSA Group
Software Engineering Institute
Carnegie Mellon University

August 2011



Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE AUG 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Analytical Evaluation Framework				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES GFIRST 2011: 7th Annual Government Forum for Incident Response and Security Teams (GFIRST) National Conference, 7-12 Aug 2011, Nashville, TN.					
14. ABSTRACT This presentation provides a framework for evaluating network traffic analysis tools.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 17	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Disclaimer

© 2011 Carnegie Mellon University

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.



Describing Network Analytical Capabilities

Develop descriptions that support fair evaluation of current or potential capabilities to address network defense needs and operational cycles

- “How does it fit” not “Is it good”
- Input to acquisition, not decision for them
- Methodical and impartial, not objective

Supportive of network security, but applicable somewhat beyond just network security

- Harvest analyst expertise
- Consideration of carry-over effects

Phase 1: A Language Model

Nouns – forms of data handled by the capability

- Inputs
- Processing
- Results

Verbs – primitive actions supported by the capability

- Data handling
- Process
- Analytic
- Presentational

Adverbs – characteristics of the capability

- Process
- Product

Prepositions – scope or limitations of the capability

Assessing Data

What is the primary data handled by the capability?

What is secondary data handled by the capability?

What is supportive data handled by the capability?

What primitive operations are associated with each?

How well are the operations implemented? What is missing?

Example: Sourcefire IDS

Primary input: Packet data

- Collect, Abstract, Parse, Alert, Store, Query, Export

Secondary input: Network map

- Select, Group, Aggregate

Supportive input: Signatures

- Import, Alert, Store, Export

Input/Processing/Output

Input: what data does the capability consume?

Sourcefire consumes network packets

Process: what data is used for control or direction of the capability?

Sourcefire uses signatures and network configuration information

Output: what data is produced by the capability?

Sourcefire produces alerts, and selective packet capture

Network Level of Abstraction

Many capabilities are focused on particular range of protocols and behaviors

IP layer: packet-based analysis, does not get into local behavior and only infers application behavior (e.g., SiLK)

Application layer: message-based analysis, does not deal with transport mechanics (e.g., analysis of email patterns)

Assessing Operations

What locus of operations forms the “core” functionality of the capability?

What are secondary operations?

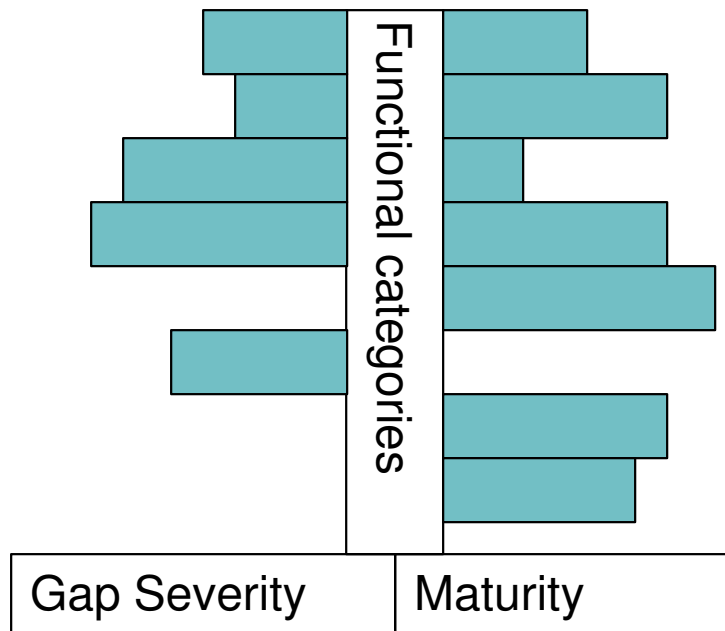
What are supportive operations?

How well are those operations implemented?

How scoped is the intended application?

Rating scheme: 0-5, plus n/a, not eval, absent

Summarizing Operational Gaps/Maturity



Balance functional maturity vs. capability gaps

All tools have gaps

Goal is to see how peaks and valleys match

Process Adverbs

Sourcefire IDS:

Operational

Qualitative

Tactical

Concise

Product Adverbs

Sourcefire IDS:

- Not Data-diverse
- Immediate
- Responsive
- Interoperable
- Documented
- Supported
- Trained
- Robust
- No Workflow
- No AAA

Prepositions

Under Conditions (e.g., edge vs. transit)

At Size / scale (e.g., enclave vs. enterprise, days vs. months)

Of Scope (e.g., CND vs. network ops)

Within Coverage (e.g., sparse vs. complete)

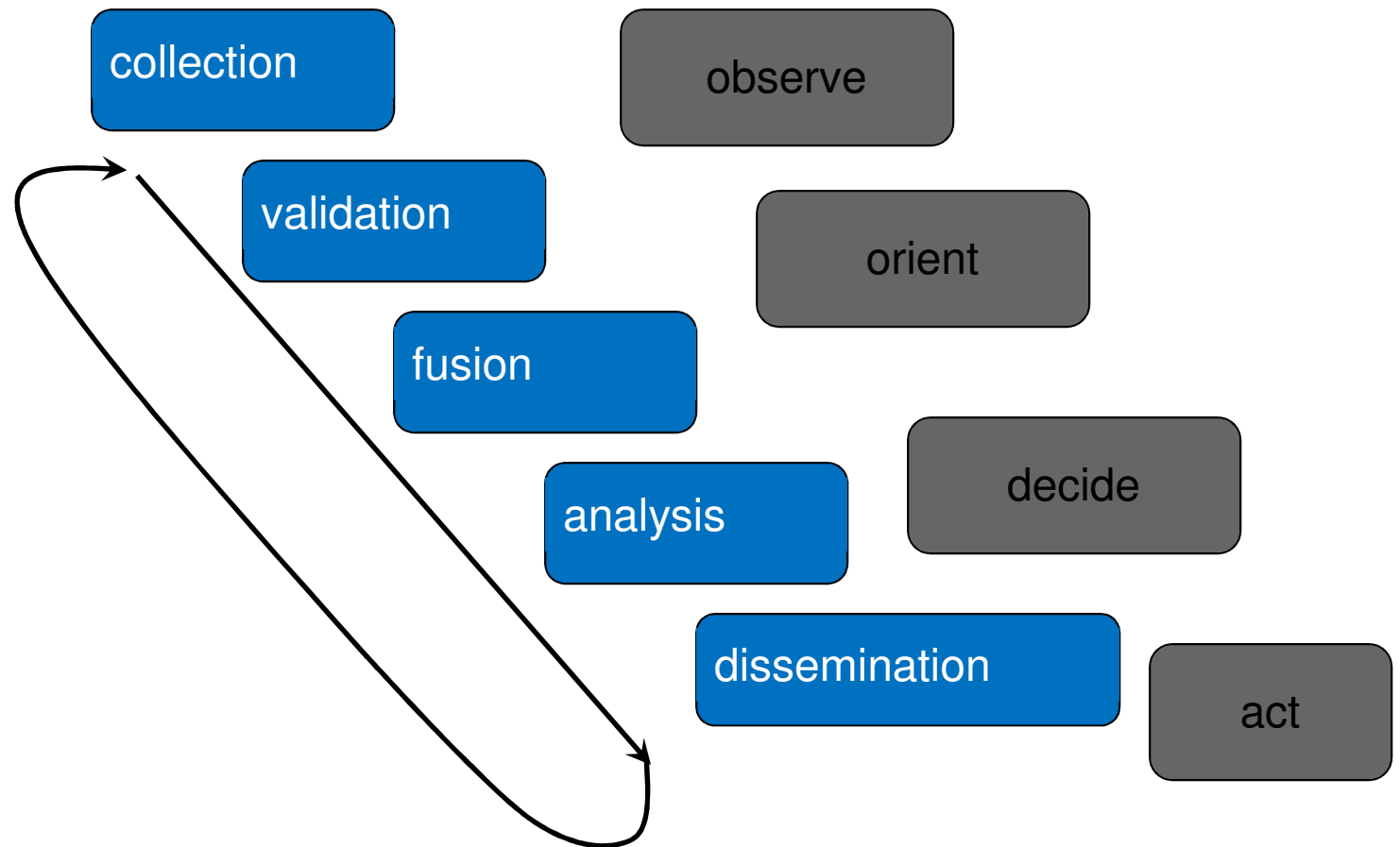
In time (e.g., interactive vs. batch vs. continuous)

Phase 2: Process Descriptions

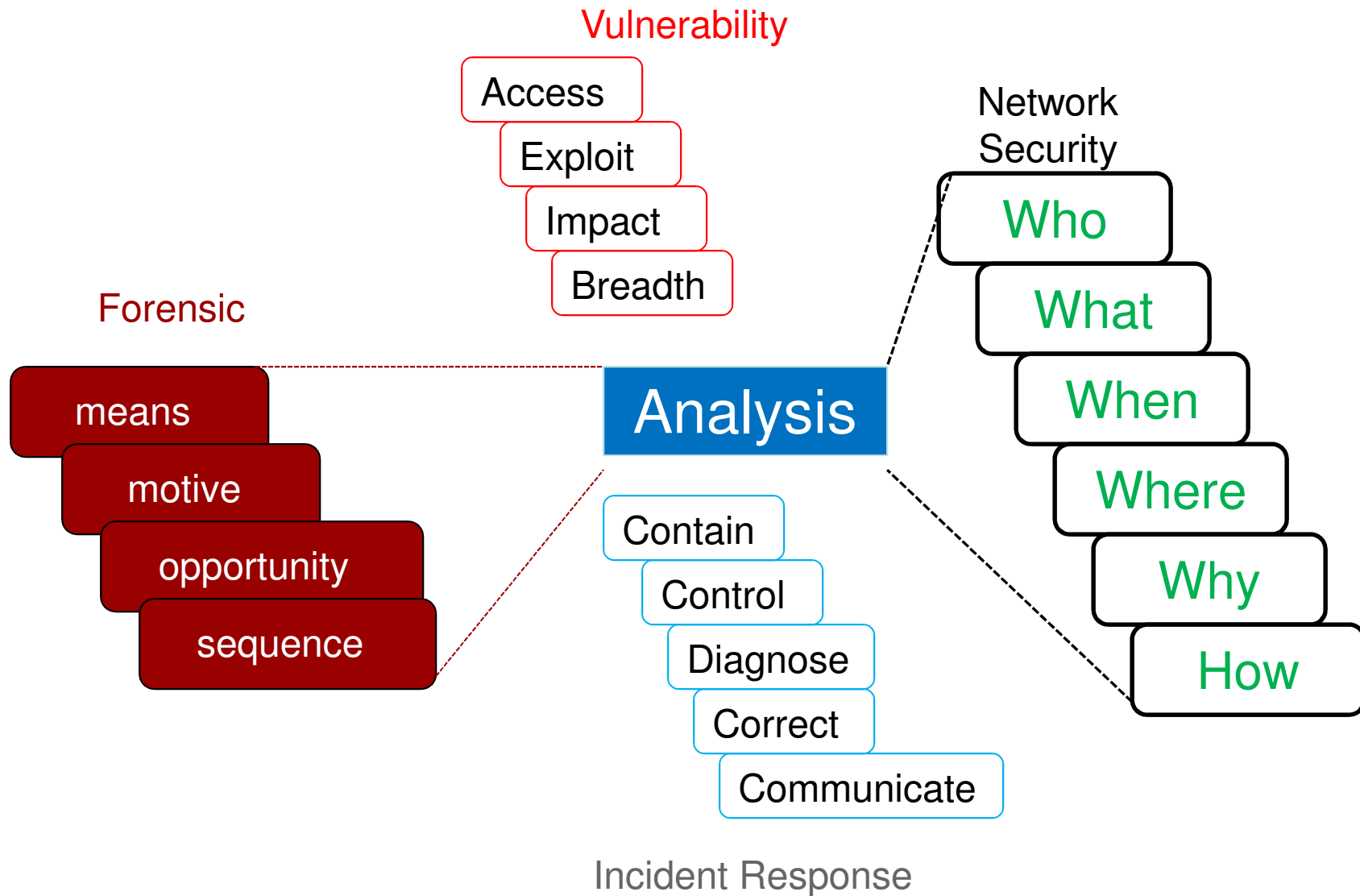
What form of reasoning should the model support?

- Fused-source intelligence
- C2/OODA?
- Forensic?
- Bayesian hypothesis testing?
- Abductive pattern matching?

Network Analysis Approaches



Analysis Decomposed



Next Steps

Expand initial visual results into fair comparisons

- Spider diagrams
- Input/Process/Output tables
- Network level tables
- Operational maturity/gaps

Define requirements for evaluation process using model

- Team?
- Approach?
- Process?
- Outcomes?
- Threats?

Tie capabilities to process needs

- Threshold approach (score needs to be X)
- Conditional approach (capability must include Y)
- Descriptive approach (need to support operations Z)

Reasoning Support