A Cognitive Study of Incident Handling Expertise

Samuel J. Perl

Richard O. Young, Ph.D.

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by DHS under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0002399

Methodology: A think-aloud study of 4 senior analysts deciding on actual incident reports

Participants: 4 cybersecurity senior analysts (experts)

Materials: 3 cybersecurity incident reports (tickets)

Data collection:

- Each expert was presented with one ticket at a time in a fixed order and asked to decide what they would recommend.
- Each expert was asked to think aloud while reading the tickets and making their decisions (Ericsson 2006, Ericsson & Simon 1993).
- Each expert's comments were recorded, transcribed, and numbered.

Data analysis: 2 coders independently coded the comments

- for the criteria the experts used to decide how to handle the incident
- for the attack attributes the experts tried to verify

Experts' think-aloud comments reveal their schemas—the info they search for to make a decision

A few of a VC's comments on a business plan

24. Telling you who their market is, is a good idea.
25. But I want to see right out front what kind of money this guy is putting up of his own.
26. I'd like to see what the tax ramifications are right up front.
27. I want to know what the project is,
28. the amount of the required investment,
29. what the tax ramifications are,
30. projected revenue and profit.

(Young 2011)

A few of Expert 2's comments on ticket 1

1. What type of activity are we looking at?
2. And then who it's from?
3. Sometimes who it's from indicates what actions I might need to take or where the information needs to go.
4. As well as who they sent it to. Did they send it just to me?
5. Or did they send it to multiple places looking for feedback from other places as well?
6. So I'm assuming the second page, this is the info that they actually sent in.

Finding 1: The experts used similar *incident handling schemas*

Incident Handling Schema Decision Criteria	Response	All 4 experts used criterion	Criterion used in all 3 tickets
1. Within expert's purview?	Y/N or Unsure	✔	✔
2. Expert's organization responsible?	Y/N or Unsure	✔	✔
3. Sender legitimate?	Y/N or Unsure	✔	✔
4. Attack serious/targeted?	Y/N or Unsure	3/4	✔
5. Attack novel/not well known?	Y/N or Unsure	✔	✔
6. Assets compromised?	Y/N or Unsure	✔	✔
7. Request for help?	Y/N or Unsure	2/4	2/3

Finding 2: The experts used similar ***attack schemas***

Attack Schema Attributes	Response	All 4 experts used attribute	Attribute used in all 3 tickets
1. Generic attack type identified?	Y/N or Unsure	✔	✔
2. Attack origin identified?	Y/N or Unsure	✔	✔
3. Network/block owner identified?	Y/N or Unsure	✔	✔
4. Target of attack identified?	Y/N or Unsure	✔	✔
5. Specific attack method/ vulnerability identified?	Y/N or Unsure	✔	✔
6. Sender's discovery method identified?	Y/N or Unsure	3/4	✔

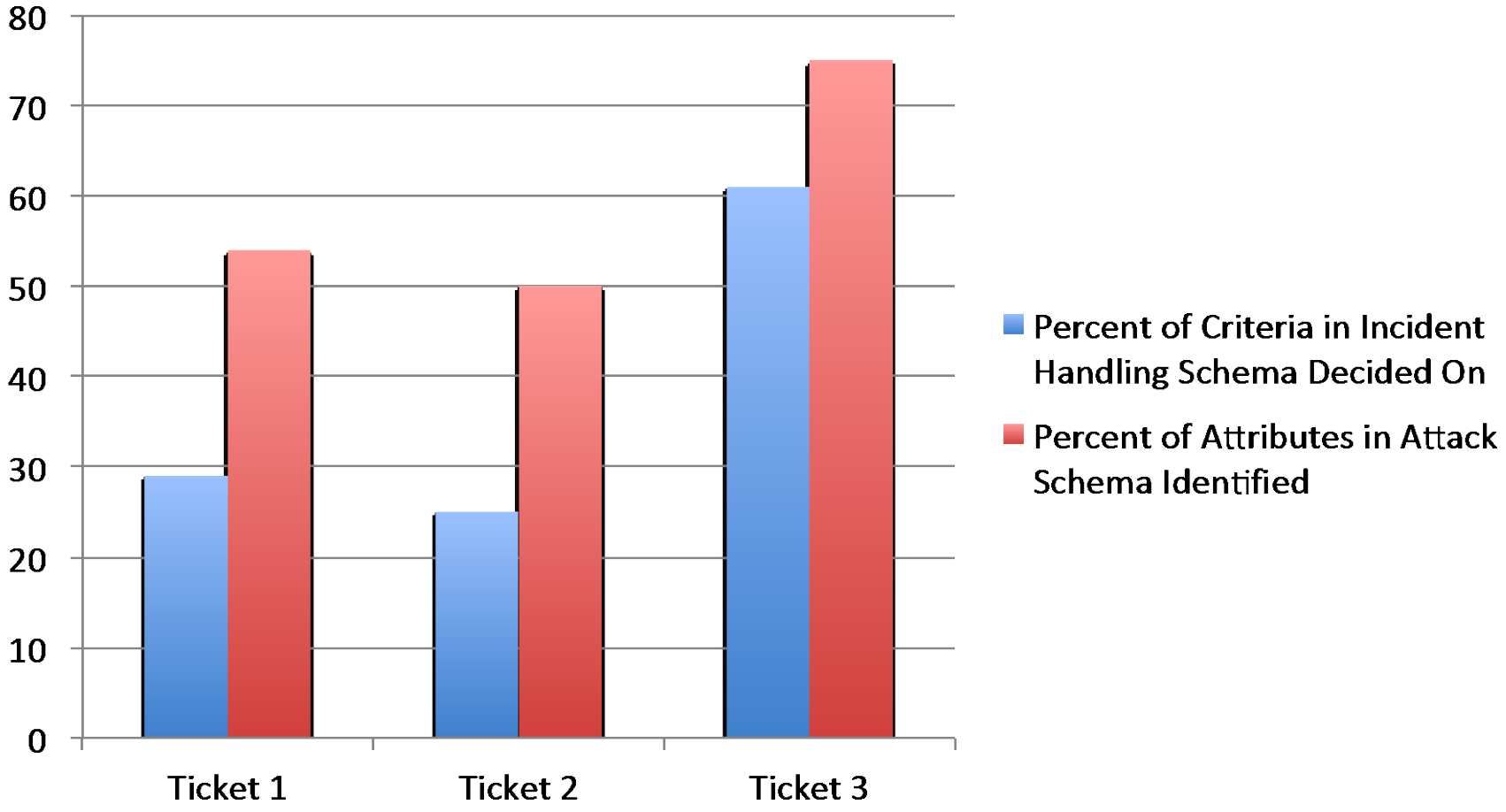
Finding 2: The experts used similar ***attack schemas***

Attack Schema Attributes	Response	All 4 experts used attribute	Attribute used in all 3 tickets
1. Generic attack type identified?	Y/N or Unsure	✔	✔
2. Attack origin identified?	Y/N or Unsure	✔	✔
3. Network/block owner identified?	Y/N or Unsure	✔	✔
4. Target of attack identified?	Y/N or Unsure	✔	✔
5. Specific attack method/ vulnerability identified?	Y/N or Unsure	✔	✔
6. Sender's discovery method identified?	Y/N or Unsure	3/4	✔

Finding 3: The experts agreed on how to handle ticket 3, but disagreed on tickets 1 and 2.

	Expert 1	Expert 2	Expert 3	Expert 4
Ticket 1 SSH Scan	TAKE NO ACTION	UNSURE HOW TO RESPOND	TAKE NO ACTION	MONITOR TARGETED MACHINES
Ticket 2 Malware	TAKE DOWN ATTACKER SITE	TAKE NO ACTION	TAKE NO ACTION	ISSUE ALERT
Ticket 3 Phishing	ISSUE ALERT	ISSUE ALERT	ISSUE ALERT	ISSUE ALERT

Finding 4: The experts found more attack attributes than incident handling criteria in the three tickets.



Finding 5: The experts' understanding of the incident in ticket 3 was most complete, definite, and in agreement.

Incident Handling Schema Decision Criteria	Ticket 1 Majority response	Ticket 2 Majority response	Ticket 3 Majority response
1. Within expert's purview?	No comment	✗	Yes
2. Expert's organization responsible?	✗	Unsure	Yes
3. Sender legitimate?	✗	Unsure	Yes
4. Attack serious/targeted?	✗	✗	✗
5. Attack novel/ not well known?	✗	Unsure	✗
6. Assets compromised?	No comment	No comment	No
7. Request for help?	✗	No comment	No comment

The format of ticket 3 prompted the sender to provide more schema-relevant information

Complete format of tickets 1 and 2

- Mail stream number:
- Spam score:
- Assignee:
- Subject:
- Date received:
- From:
- To:
- CC:
- Replication:

Partial format of ticket 3 (8 of 48 questions)

- Tracking number:
- Report type:
- Contact information:
- Reporting date:
- Reporting tier:
- Categories:
- Explain how the tier/categories were determined:
- Impact from this incident:

Hypothesis: The experts' agreement on ticket 3 depended on the structured format used by the sender

Incident Handling Schema Decision Criteria	Unstructured Format (Tickets 1 & 2) Criterion requested by form or inferable from it	Structured Format (Ticket 3) Criterion requested by form or inferable from it
1. Within expert's purview?	✗	✔
2. Expert's organization responsible?	✗	✔
3. Sender legitimate?	✗	✔
4. Attack serious/targeted?	✗	✔
5. Attack novel/ not well known?	✗	✔
6. Assets compromised?	✗	✔
7. Request for help?	✗	✔

Discussion: Our findings and hypothesis are consistent with findings in many different fields

- Expertise has been shown to be schema-driven among:
  - accountants (Bhaskar 1978)
  - physicists (Larkin, McDermott, Simon, & Simon 1980)
  - medical doctors (Heller, Saltzstein, & Caspe 1992)
  - Wall Street analysts (Kuperman 2000)
  - military officiers (Connely et al. 2000)

- Although experts' decisions show a high degree of consensus in some fields, consensus is low in most (Shanteau 1992; Stewart, Roebber, & Bosart 1997).

High consensus	Low consensus
Weather forecasters	Pathologists
Actuaries	Clinical psychologists
Physicists	Stockbrokers

- Decision quality in law, finance, and military operations has been shown to suffer when schema-relevant information is missing or when it is not formatted in a way that reflects experts' schemas (Baranski & Petrusic 2010; Brenner, Koehler, & Tversky 1996; Maines & McDaniel 2000; Young 2011).

Recommendations

1. Provide **senders** with a structured format to fill in that reflects the experts' schemas.

2. Provide **junior analysts** with a structured format to fill in that reflects the experts' schemas.

3. Provide **senior analysts** with a mobile app that tracks their schema-driven analysis.

References

- Bhaskar, R. (1978). Problem solving in semantically rich domains (Doctoral dissertation, Carnegie Mellon University, 1978). *Dissertation Abstracts International*, *41* (05B), 1826.
- Baranski, J. V., Petrusic, W. M. (2010). Aggregating conclusive and inconclusive information: Data and a model based on the assessment of threat. *Journal of Behavioral Decision Making , 23*(4), 383-403.
- Brenner, L. A., Koehler, D. J., Tversky, A. (1996). On the evaluation of one-sided evidence*. Journal of Behavioral Decision Making , 9*(1), 59-70.
- Connelly, M. S., Gilbert, J. A., Zaccaro, S. J., Threlfall, K. V., Marks, M. A., & Mumford, M. D. (2000). Exploring the relationship of leadership skills and knowledge to leader performance. *Leadership Quarterly, 11*, 65–86.
- Ericsson, K. A. (2006). Protocol analysis and expert thought: Concurrent verbalizations of thinking during experts' performance on representative tasks. In K. A. Ericsson, N. Charness, P. Feltovich, & R. Hoffman (Eds.), *The Cambridge handbook of expertise and expert performance* (pp. 223–241). Cambridge, UK: Cambridge University Press.
- Ericsson, K. A., & Simon, H. A. (1993). *Protocol analysis: Verbal reports as data* (revised edition). Cambridge, MA: Bradford Books/MIT Press.
- Heller, R. F., Saltzstein, H. D., & Caspe, W. B. (1992). Heuristics in medical and non-medical decision-making. *The Quarterly Journal of Experimental Psychology A: Human Experimental Psychology*, *44A*(2), 211–235.
- Kuperman, J. C. (2000). Financial analyst sensemaking following strategic announcements: Implications for the investor relations activities of firms (Doctoral dissertation, New York University, 2000). *Dissertation Abstracts International*, *61* (05A), 1936.
- Larkin, J. H., McDermott, J., Simon, D. P., & Simon, H. A. (1980). Models of competence in solving physics problems. *Cognitive Science*, *4*(4), 317–345.
- Maines, L. A., & McDaniel, L. S. (2000). Effects of comprehensive-income characteristics on nonprofessional investors' judgments: The role of financial-statement presentation format. *The Accounting Review*, *75*(2), 79–207.
- Shanteau, J. (1992). Competence in experts: The role of task characteristics. *Organizational Behavior and Human Decision Processes Special Issue: Experts and Expert Systems*, *53*(2), 252–266.
- Stewart, T. R., Roebber, P. J., & Bosart, L. F. (1997). The Importance of the Task in Analyzing Expert Judgment. *Organizational Behavior and Human Decision Processes, 69* (3), 205-219.
- Young, R. O. (2011). How audiences decide: A cognitive approach to business communication. New York: Routledge.

Contact Information

Samuel J. Perl

Carnegie Mellon University
Software Engineering Institute
CERT Program

4500 Fifth Avenue
Pittsburgh, PA, 15213

sjperl@cert.org

Richard O. Young, Ph.D.

Carnegie Mellon University
Tepper School of Business

5000 Forbes Avenue
Pittsburgh, PA, 15213

ry02@andrew.cmu.edu