Practicing a Science of Security: Reflections

Jonathan M. Spring

Based on joint work with Tyler Moore, David Pym, Phyllis Illari, and Eric Hatleback

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM19-0038

Outline

History of the philosophy of science

- I promise this will be short and useful

ACoD CFP and philosophy of science in practice

- AKA, translating between technical and PhilSci problems

Audience participation

- What technical topics and challenges would most benefit from/to PhilSci?

History of the philosophy of science

For the full story, see our paper: “Practicing a Science of Security: A philosophy of science approach”

Super-simplified version:

1. (1920s) Physics is super confusing now
2. (1930s-1950s) Science = evidencing physical laws of nature
3. (1960s-2000s) JK, that’s silly, science is a complicated social phenomenon outputting integrated but plural overlapping non-reducible models / explanations
4. (2010s) Some people complain computer security doesn’t have laws of nature so it’s not a science
    - I’m confused as to why they ignore #3

CFP

Happily, the ACoD organizers are brilliant and did a better job

“Push the Art to a Science: …To mature our practice, we need to be able to share our methodologies in a systematic and consistent way… We'd like to philosophically discuss concepts in security, push them forward, and model them.”

We cite this in the 2017 paper as promising but too early to tell

I’m basically here to follow up on that.

Specifically, I can help with “share our methodologies in a systematic and consistent way”

Systematic and Consistent

Let's call this a cluster of three questions:

- What does general knowledge look like?
- How do we collect evidence for general knowledge?
- When do we know we have reliable / stable knowledge?

Roughly, I can say

1. See our paper "Building General Knowledge of Mechanisms in Information Security"
2. Experiments and structured observations and science (See "Practicing a Science of Security" paper)
3. ¯_(ツ)_/¯ … Consensus?

Hypothesis!

Good threat intelligence explanations ≈ good scientific explanations

No one else, as far as I know, publishes on this in academic circles

Closest advice might be philosophy of science in practice

Philosophy of Science in Practice

http://www.philosophy-science-practice.org/

1. “We are concerned with not only the acquisition and validation of knowledge, but its use. …We aim to build meaningful bridges between the philosophy of science and the newer fields of philosophy of technology and philosophy of medicine...
2. “…We seek to elucidate the role that [artifacts such as conceptual models and laboratory instruments] play in the shaping of scientific practice.
3. “Our view of scientific practice must not be distorted by lopsided attention to certain areas of science…
4. “In our methodology, it is crucial to have a productive interaction between philosophical reasoning and a study of actual scientific practices, past and present. ...”

Audience Participation

What are the features of infosec that interfere with your structured observations?

Trading zones

In anthropology, we think of trading zones as a physical space that is built up to allow exchange

But its also languages and skills

Galison applies this concept to scientific specialties

I'd like to build up a trading zone between infosec practice and philsci, where we can translate

Audience Participation

What are the features of infosec that make maturing the practice of infosec hard?

Which of these features are shared with relatively few other fields?

Which features are shared widely?

- (so we can borrow advice instead of reinventing it)

Questions?

Thank you for your time

Feel free to reach out: jspring at the domain cert.org

If you want further philosophy of science reading, this is a review:

Spring JM, Moore T, Pym D. Practicing a science of security: A philosophy of science perspective. New Security Paradigms Workshop. 2017 Oct 1

https://tylermoore.utulsa.edu/nspw17.pdf