Science, Security, and Academic Literature: Can We Learn from History?

Paul C. van Oorschot
Carleton University, Ottawa, Canada

ABSTRACT

A recent paper (Oakland 2017) discussed science and security research in the context of the government-funded Science of Security movement, and the history and prospects of security as a scientific pursuit. It drew on literature from within the security research community, and mature history and philosophy of science literature. The paper sparked debate in numerous organizations and the security community. Here we consider some of the main ideas, provide a summary list of relevant literature, and encourage discussion within the Moving Target Defense (MTD) sub-community.[1]

CCS CONCEPTS

• **General and reference** → **Experimentation**; Empirical studies; Evaluation; • **Security and privacy** → *Formal security models*; *Systems security*;

KEYWORDS

science of security, cybersecurity research, limitations of models, induction, deduction, empirical research

INTRODUCTION

A recent Oakland paper [14] on the topic of science and security research, co-authored with Cormac Herley, explores a number of issues of direct interest to the community studying problems under the Moving Target Defense (MTD) banner. These include differences between those who value theory and information theoretic metrics over empirical work, data collection and real-world experiments—and vice versa.[2] There is lack of consensus on what a sound scientific methodology should entail. This note and accompanying talk aim to relate and extend the discussion of science and security to the MTD workshop, and to promote further discussion.

On learning from history, rather than about security details, the questions are: how to carry out research, what methodologies to use, what goals to set, where the opportunities for improvement are, and which aspects of traditional science can help computer and Internet security research.

[1] This note accompanies a keynote talk for the MTD'17 workshop held in conjunction with ACM CCS 2017.
[2] I thank the MTD'17 co-chairs for this characterization/motivation.

MTD'17, October 30, 2017, Dallas, TX, USA.

ACM ISBN 978-1-4503-5176-8/17/10.
https://doi.org/10.1145/3140549.3140563

SOME MAIN IDEAS

The Oakland SoK [14] selectively reviewed science literature and security-specific literature, and highlighted areas where the security community was failing to follow scientific principles and methodologies, or to leverage lessons long-known in other sciences. Some of the main ideas are summarized below, along with recommended references.

1. Deduction and induction: Some research involves formal methods, and results proven as logical consequences of axioms plus starting conditions. Work exclusively in this *deductive* realm offers a strange bargain: it can give 100% guarantees in the mathematical sense of proofs, but since it is blind on whether the starting conditions hold in the real world, the same is true for the results. An *assumption* that starting conditions hold, plus formally deducing the consequences, is not a "proof" that results hold in the real world; that depends on the (untested) assumption. Purely deductive reasoning without empirical validation precludes corrective feedback uncovering errors in modelling or reasoning. While mathematics and logical reasoning are valuable tools, science requires contact with the observable world. *Induction* allows moving from specific observations to general results and broader understandings; it is more intuitive, often relying in part on deductive reasoning. It also has a disadvantage: it lacks 100% guarantees. See Ayer [2] for a clear discussion of the inductive and deductive realms—and also the dangers of misleading language and terminology. A security example of the latter is *provable security*; this term reliably leads to confusion [6, 17] between security researchers and cryptographers, and between cryptographers and mathematicians [16].

2. Limits of models: George Box gets credit for the aphorism: *All models are wrong but some are useful.* Models aid reasoning and understanding. Results derived from models do not, a priori, extend to the real word. Some will, and some won't (e.g., due to invalid assumptions). Establishing the validy of assumptions, and that models accurately represent the real world (or its man-made computer artifacts), is itself an empirical task that can not be proven deductively. Any "proof" that results from a model hold in the real world would involve explicitly writing down all assumptions and convincingly testing their validity in the target real-world environment; it would also require the meta-assumption of no missing assumptions, itself problematic (see Dashti [5]). For insightful discussion of the relationship between formal models and reality, see Denning [8] and Schaefer [31]. Younger researchers are encouraged to read about the 1980s-era confusion on what exactly the Bell-LaPadula model modelled [3, 24–26]. Ensuing self-reflection and calls for establishing computer security foundations [13, 32] sound eerily familiar.

3. Limits of formal verification: Formal verification means not an absence of security problems, but rather that some carefully specified list of properties has been formally shown. Many things could still go wrong, including due to as-yet-unknown classes of vulnerabilities—which are especially difficult to prove immunity against, as are all vulnerabilities outside of a fixed security model being used (as *side channel* attacks often are). Too often, once the words "formally verified" are spoken, the questions stop. Unasked is: *With respect to what subset of security properties?* Much progress in formal verification has been made—consider seL4 [11], and TLS (see Oakland 2017 proceedings). But also re-read DeMillo et al. [7], and ask which 1979 issues remain open.

4. Security is different: This excuse sometimes arises on asking: where is the science in security? Many sciences have unique challenges. Experiments controlling planetary motion are expensive—so astronomers instead rely on observation. While many aspects of physics are constant, life sciences face evolving diseases. Whatever unique characteristics of security exist, they should not prevent researchers from leveraging scientific principles and methodologies where beneficial.

5. What is science? There are many views. Science involves understanding the world; facts, distinct from theorems, involve statements about the physical world. For the defining characteristics of science, see introductory philosphy of science books (e.g., [4], [12]). On how computer science measures up, see Denning [9]. Platt's idea of *strong inference* [29] is important. Feynman's essays [10] convey a physicist's view. Science may involve long sequences of iteratively improving understanding, followed by models being entirely abandoned—Kuhn [18] describes paradigm shifts and scientific revolutions. Popper is known for *falsification* [30]. Computer science is what Herbert Simon calls a *science of the artificial* [34]—much of what is studied is not the natural world, but human artifacts. Science is about methodologies; those used in the hard sciences differ from those used in, e.g., biology—consider Darwin [1]. Science is also about priorities and goals—for example, government sponsors of security have explored how many funded projects result in commercial products [22]. With an eye on the public benefit of science funding, Stokes [35] promoted *Pasteur's Quadrant*, a model whose exemplars did not pit pure research against applied, but rather supported both, placing high value on advancing both fundamental knowledge and considerations of practical use.

6. Science of Security literature: The Science of Security movement is largely due to government funding, including the NSA [27, 28]. The JASON group report [15] is recommended background, albeit emphasizing formal methodologies over systems security. Landwehr [19] gives an insightful view of the role of engineering. Shostack [33] reminds us to stay grounded in practice. Other circa-2010 efforts to understand why there has not been a stronger connection between security and science include Maxion's panel [23], and Longstaff [20, 21], who is among others to observe that many security researchers have very little training in science itself. A first step is to read enough to understand how little you know; a second step is to improve scientific training for security researchers.

REFERENCES

[1] Francisco J Ayala. 2009. Darwin and the scientific method. *Proc. National Acad Sciences* 106, Supplement 1 (2009), 10033–10039.

[2] Alfred Jules Ayer. 2014. *Language, Truth and Logic*. Dover Publications, New York (unaltered reproduction of 2/e, 1946).

[3] David Elliott Bell. 1988. Concerning 'modeling' of computer security. In *IEEE Symp. Security and Privacy*. 8–13.

[4] Alan F Chalmers. 2013. *What is this thing called Science? (4th edition)*. Hackett Publishing.

[5] Mohammad Torabi Dashti and David A. Basin. 2016. Security Testing Beyond Functional Tests. In *Proc. ESSoS (Eng. Secure Software and Systems) (Springer LNCS 9639)*. 1–19.

[6] J P Degabriele, K Paterson, and G Watson. 2011. Provable security in the real world. *IEEE Sec & Priv* 3, 9 (2011), 33–41.

[7] Richard A. DeMillo, Richard J. Lipton, and Alan J. Perlis. 1979. Social Processes and Proofs of Theorems and Programs. *Commun. ACM* 22, 5 (1979), 271–280. See also C.ACM 22(11):621–630.

[8] Dorothy Denning. 1999. The limits of formal security models. *Nat Computer Sys Security Award. Acceptance speech* (1999).

[9] Peter J. Denning. 2013. The Science in Computer Science. *Commun. ACM* 56, 5 (2013), 35–38.

[10] Richard P Feynman. 2010. *"Surely You're Joking, Mr. Feynman!": Adventures of a Curious Character*. Norton & Co.

[11] Gerwin Klein et al. 2009. seL4: formal verification of an OS kernel. In *Proc. SOSP*. ACM, 207–220.

[12] Peter Godfrey-Smith. 2009. *Theory and reality: An introduction to the philosophy of science*. University of Chicago Press.

[13] Donald I. Good. 1986. The Foundations of Computer Security: We Need Some. (1986). Essay.

[14] Cormac Herley and Paul C. van Oorschot. 2017. SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit. In *IEEE Symp. Security and Privacy*. 99–120.

[15] JASON Program Office, Report JSR-10-102. 2010. Science of Cyber-security. (2010).

[16] Neal Koblitz. 2007. The uneasy relationship between mathematics and cryptography. *Notices of the AMS* 54, 8 (2007), 972–979.

[17] Neal Koblitz and Alfred Menezes. 2007. Another Look at 'Provable Security'. *J. Cryptology* 20, 1 (2007), 3–37.

[18] Thomas S Kuhn. 1962. *The Structure of Scientific Revolutions*. University of Chicago Press (first edition).

[19] Carl Landwehr. 2012. Cybersecurity: From engineering to science. (2012), 2–5. In [28].

[20] Tom Longstaff. 2012. Barriers to achieving a science of cybersecurity. (2012), 14–15. In [27]; talk transcript (15 Mar 2012) at https://www.nsf.gov/attachments/123376/public/transcript.pdf.

[21] Tom Longstaff, David Balenson, and Mark Matties. 2010. Barriers to science in security. In *Proc. ACSAC*. ACM, 127–129.

[22] D Maughan, David B, U Lindqvist, and Z Tudor. 2013. Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice. *IEEE Security & Privacy* 11, 2 (2013), 14–23.

[23] R A Maxion, T A Longstaff, and J McHugh. 2010. Why is there no science in cyber science? (panel). In *Proc. NSPW*. ACM, 1–6.

[24] John McLean. 1985. A Comment on the 'Basic Security Theorem' of Bell and LaPadula. *Inf. Process. Lett.* 20, 2 (1985), 67–70.

[25] John McLean. 1987. Reasoning About Security Models. In *Proc. IEEE Symp. Security and Privacy*. 123–133.

[26] John McLean. 1990. The Specification and Modeling of Computer Security. *IEEE Computer* 23, 1 (1990), 9–16.

[27] NSA. 2012. Building a national program for cybersecurity science. *The Next Wave* (2012). vol.19, no.4.

[28] NSA. 2012. Developing a blueprint for a science of cybersecurity. *The Next Wave* (2012). vol.19, no.2.

[29] J.R. Platt. 1964. Strong inference. *Science* 146, 3642 (1964), 347–353.

[30] Karl Popper. 1959. *Conjectures and refutations: The growth of scientific knowledge*. Routledge.

[31] Marvin Schaefer. 1989. Symbol Security Condition Considered Harmful. In *Proc. IEEE Symp. Security and Privacy*. 20–46.

[32] Marvin Schaefer. 1993. We Need to Think About the Foundations of Computer Security. In *Proc. NSPW*. ACM, 120–125.

[33] Adam Shostack. 2012. The evolution of information security. (2012), 6–11. In [28].

[34] Herbert A Simon. 1996. *The Sciences of the Artificial*. MIT Press, Cambridge, MA (third edition; originally published 1969).

[35] Donald E Stokes. 1997. *Pasteur's Quadrant: Basic Science and Technological Innovation*. Brookings Institution Press.