

Helsinki-Aalto Center for Information Security: HAIC talk
Aalto University – 20 June 2018

**Science of Security:
Theory vs.
Measuring the Observable World**

(joint work with Cormac Herley, MSR)

Paul Van Oorschot

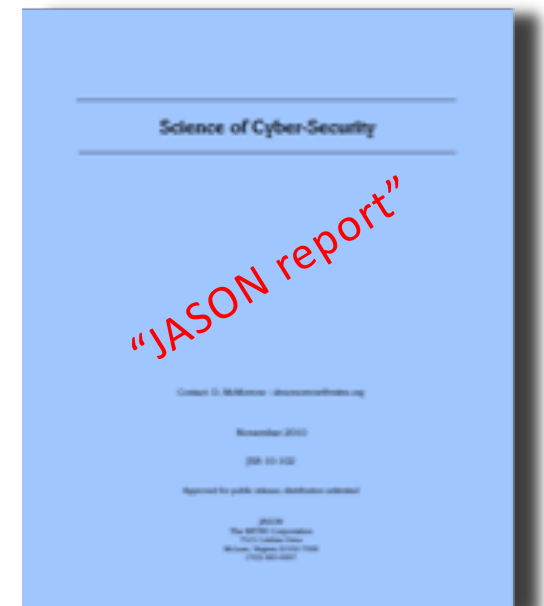
Professor of Computer Science – Carleton University, Ottawa
Canada Research Chair in Authentication & Computer Security

Science of Security

- NSA-sponsored activity (2008)
- JASON report (DoD, 2010); formal methods
- NAS Foundational Cybersecurity Research (2017)
 - “high-level roadmap” considering “research goals & directions for foundational science in cybersecurity”

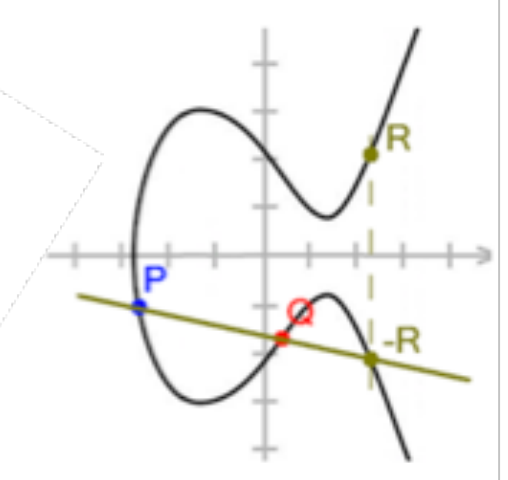


Underlying motivation?



What do we mean by “Science”?

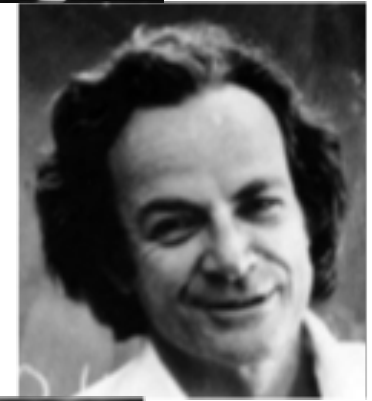
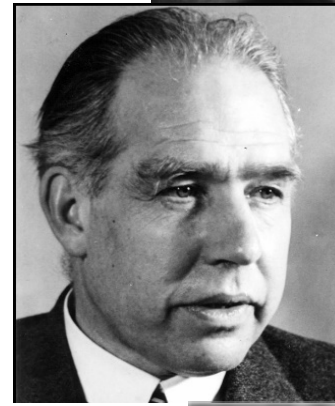
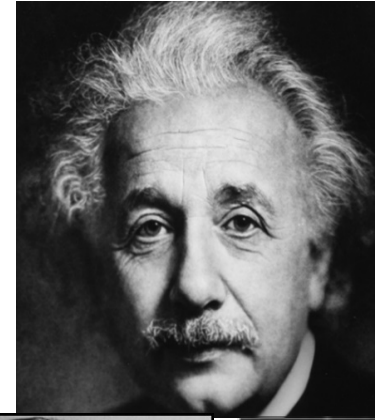
- Equations?
- Numbers and Graphs?
- Repeatable experiments?
- Rigor? Proofs?



P.J. Denning (CACM 2013),
“The science in computer science”

$$E = mc^2$$

Philosophy/History of Science



- Chalmers (2013, 4/e). *What is this thing called Science?*
- Godfrey-Smith (2009). *Theory and reality: An introduction to philosophy of science*

What are a few consensus items from other fields?

If theory conflicts with observation: the theory is wrong.

Conflict with observation must actually be possible.

Science requires induction, not deduction alone.

Claims must be falsifiable.



Falsifiability

“A theory which is not refutable by any conceivable event is non-scientific.

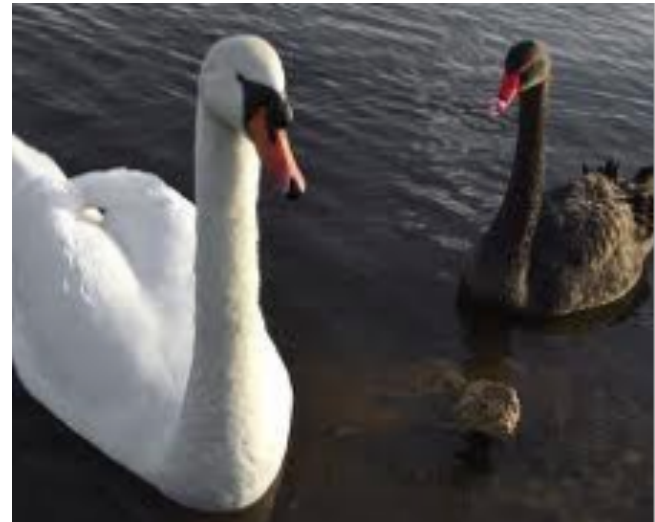
Irrefutability is not a virtue of a theory (as people often think) but a vice.”

-K. Popper

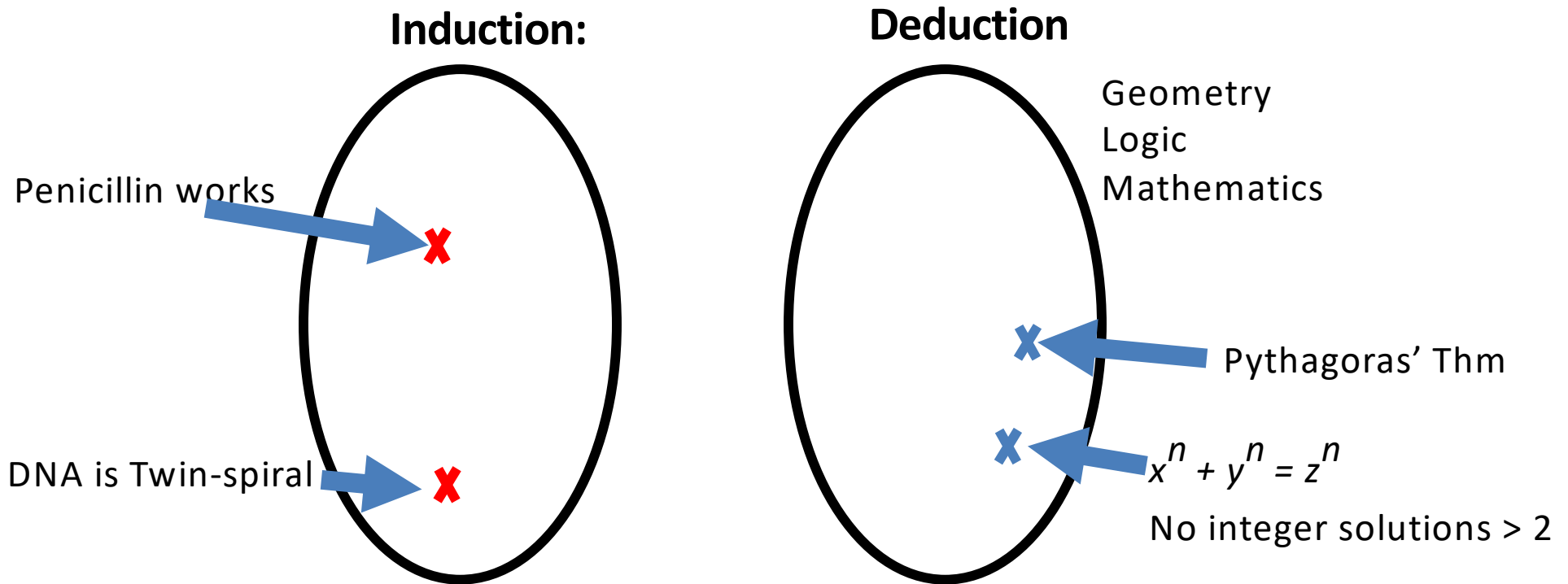
If: X cannot be falsified by any observation

Then: X is consistent with every possible observation.

⇒ nothing observable depends on X
(observation tells nothing about X)

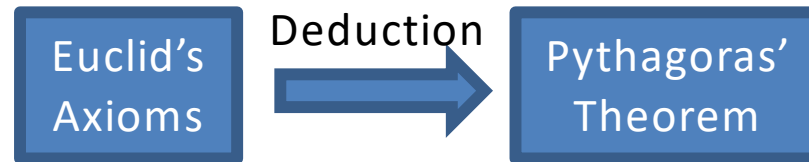


- **Induction:** statements about real world
 - moving from specific observations to general results
- **Deduction:** proved-true statements from axioms



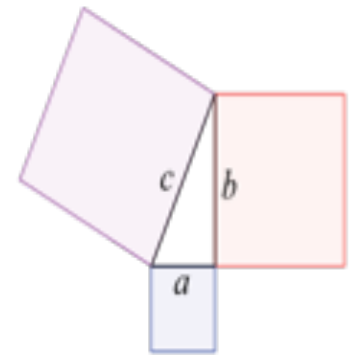
	Inductive Statements	Deductive Statements
Describe real-world?	Yes	No
Certainty?	Always uncertain	100% confidence
Believe when:	Try to falsify and fail	Have a proof

So ... Math isn't Science???



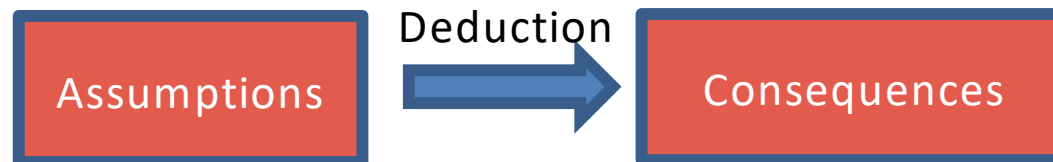
No observation contradicts Pythagoras' Thm

- If $a^2 + b^2 \neq c^2$ on measuring door, we do not say the theorem is wrong



Axiom: parallel lines meet at infinity

Assumption: attacker can't take finite field logs



Observations contradicting assumptions are possible.
Scientific claims retain uncertainty.

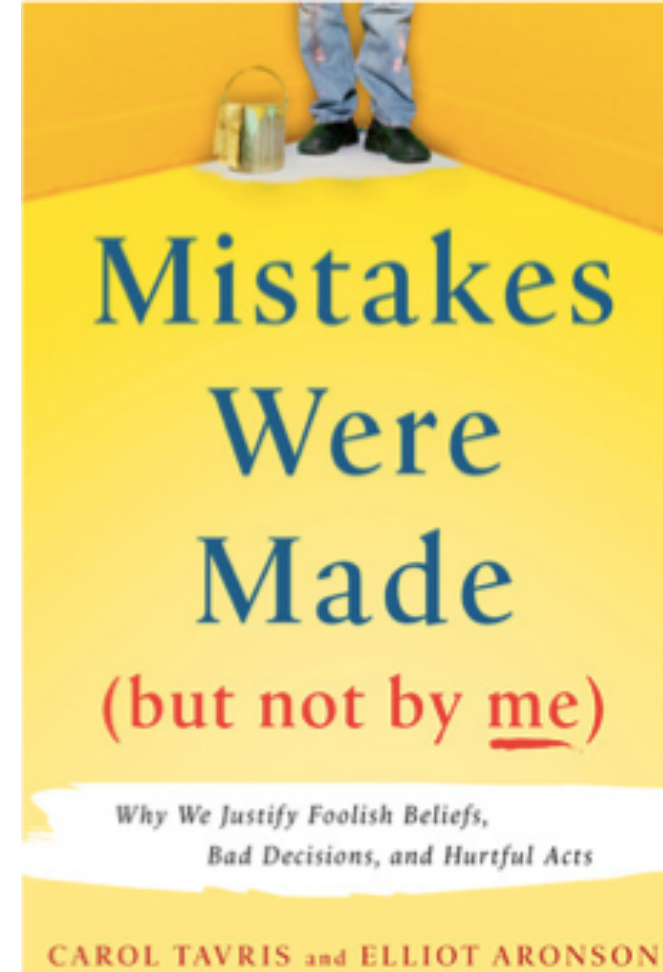


. . . What
does any of this
have to do with
security?

**BREAKING
NEWS**

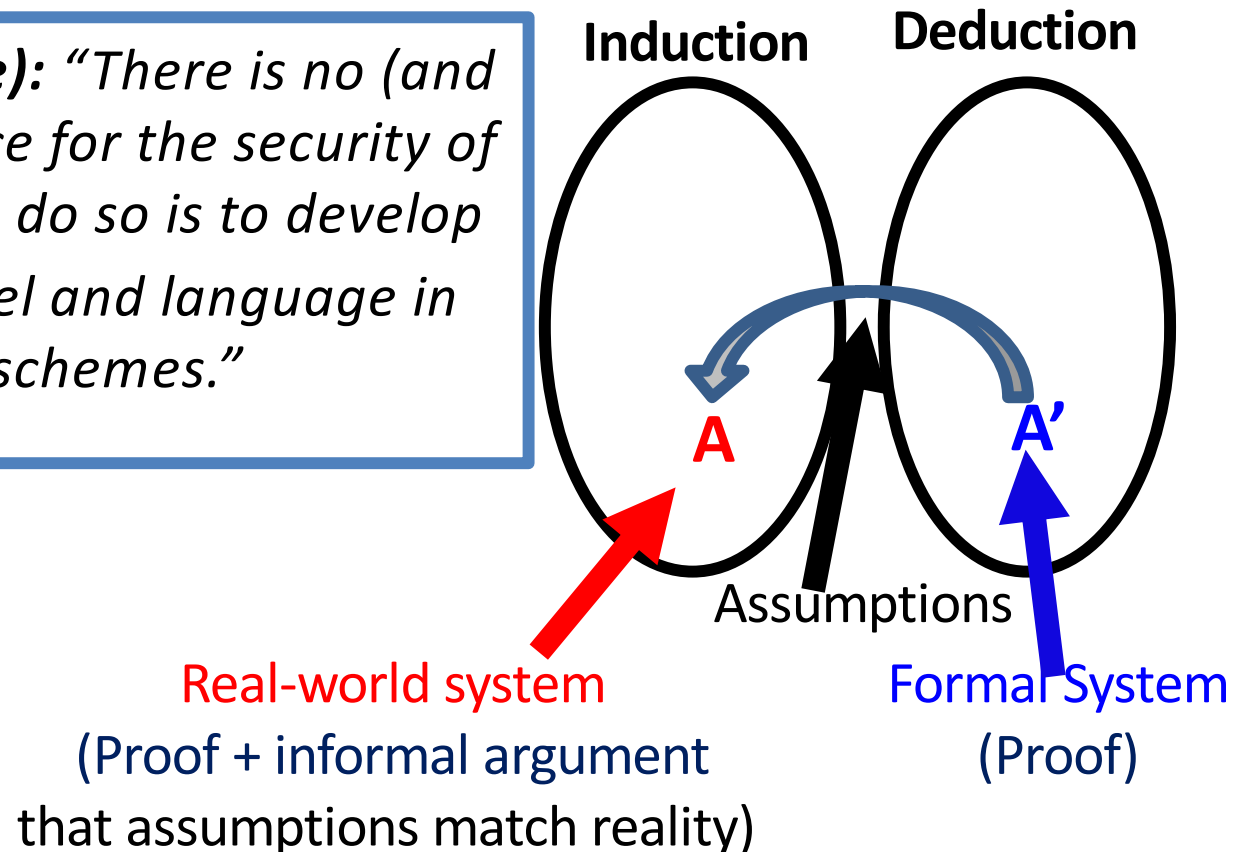
Not everything
is perfect
in security research...

[A few examples follow]



1. Failure to separate Induction/Deduction

Problematic Claim (example): “There is no (and cannot be) empirical evidence for the security of a design [...] The only way to do so is to develop a formal mathematical model and language in which to reason about such schemes.”

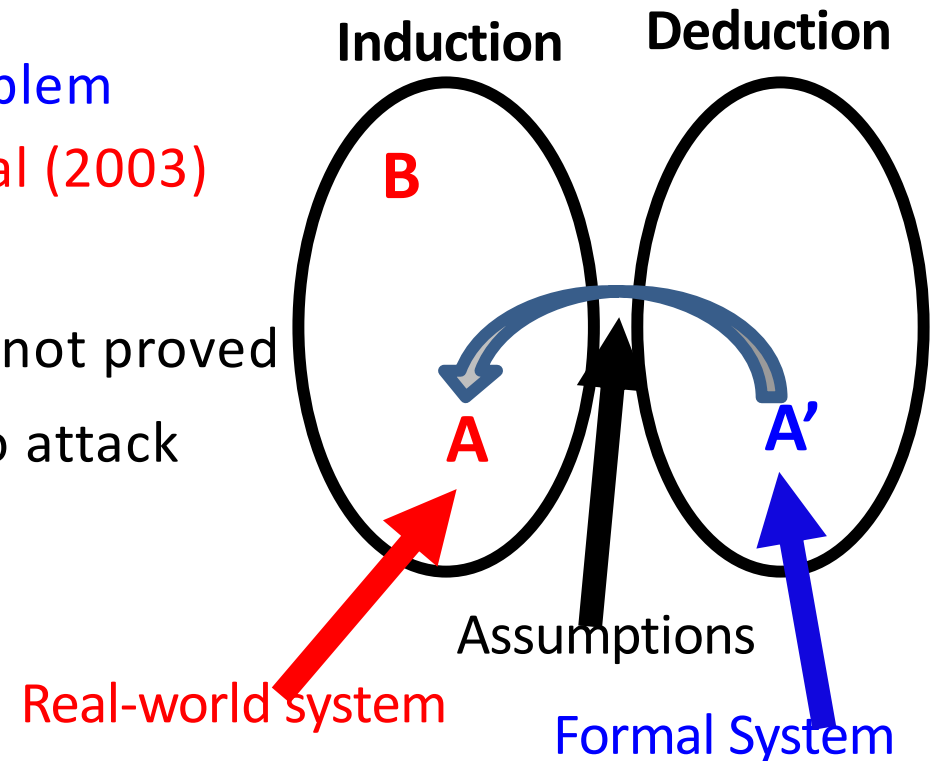


That a real-world system satisfies stated assumptions is an empirical claim, that cannot be proven by abstract reasoning.

1. Failure to separate Induction/Deduction [cont'd]

Example:

- **A'**: attack on TLS must solve hard problem
- **A**: Remote Timing Attacks are Practical (2003)
- **A** enjoys properties of **A'** is assumed, not proved
- No possibility of *proving* **A** immune to attack



(proof + paragraph about assumptions being reasonable) ≠ (a proof)

The real world's messy details can't be "proven away" by magical wands or any other means (including deduction)

Side note: “Reasonableness of assumptions”
is no substitute for testing against observation

Newton: speed of fall in a vacuum = $g \cdot t$

- air pressure $\neq 0$; but we rely because predictions accurate



“Reasonable” is subjective; not an alternative to empirical testing

Deduction can reveal logical consequences of premises/axioms

- but can't help determine if assumptions match reality



butter

substitute by



mashed avocado

2. Failure to bring theory into contact with observation

“Passwords should contain a mix of upper, lower & special chars”

- Morris & Thompson, 1979

For 30-35 yrs it was ***assumed*** that complex password composition rules lead to better guess-resistance in practice. But:

- Do we have real-world A/B tests?
- Observations of *improved outcomes*?

What observational evidence supports the claim:

- *that passwords should be changed every 90 days:*



3. Reliance on Unfalsifiable Claims

It's not possible to "observe" that a real-world system is secure. So it's unfalsifiable to claim that a real-world system is insecure.

- falsifying would require observing that a system is secure
- claims of necessary conditions for real-world security unfalsifiable

"If you don't do X you are not secure" is unfalsifiable for all X

- example X: choose a password that withstands 10^{14} guesses



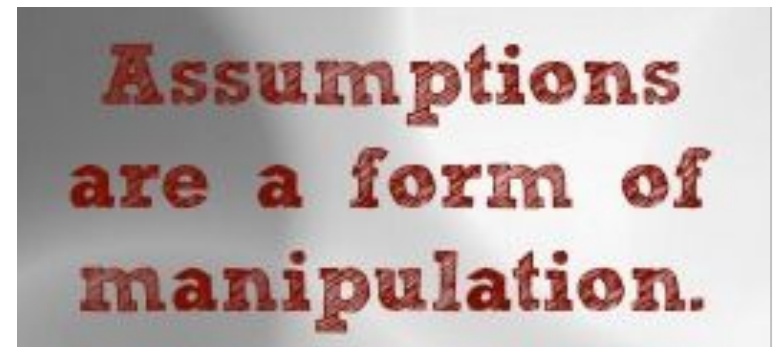
4. Reliance on implicit/unstated assumptions

Universal agreement: assumptions should be clearly stated.

So what is the precise list of assumptions to justify that:

- complex password composition policies improve outcomes

Hard to falsify assumptions that we (can't or) haven't even listed



**Assumptions
are a form of
manipulation.**

So what should we do
about this?



T1: Clearly define desired aspects of Science

*Pushes for “more science” in security,
that rule nothing in or out,
are too ambiguous to be effective.*

*Many insights and methods from philosophy of science
remain largely unexplored in security research.*



- existing exhortations to be more scientific are circular
- simply declaring a desire for more “Science” is unhelpful



T2: Acknowledge the inductive-deductive split

Ignoring the sharp distinction between inductive and deductive statements is a consistent source of confusion in security.

- all scientific statements contain uncertainty
- absolute guarantees necessarily remain in deductive realms



T3: Stop relying on unfalsifiable claims

*Unfalsifiable claims are common in security
– and along with circular arguments,
are used to justify many defensive measures
in place of evidence of efficacy.*

“Falsification is the engine
of self-correction” (Popper)



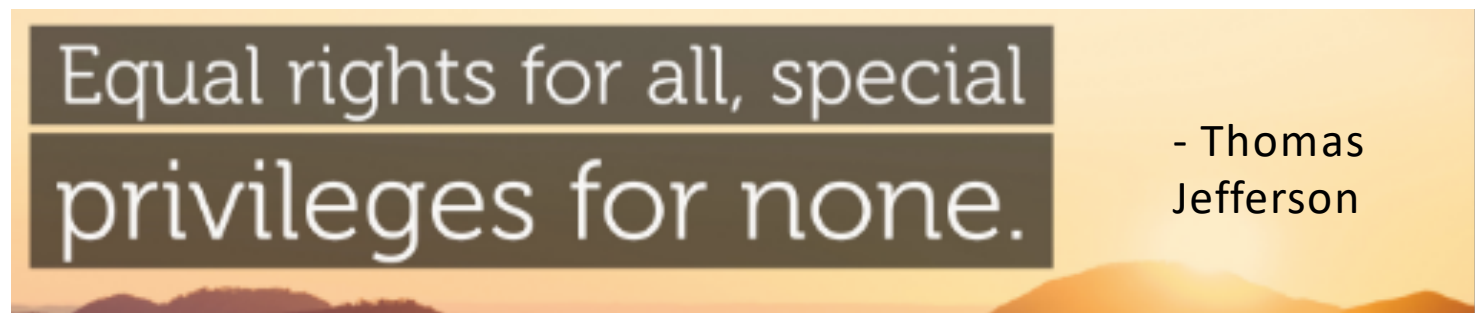
- Does inability to “observe” security doom efforts for a Science?
 - focus on observable outcomes (vs. ambiguous words like “secure”)
 - be explicit: specific attacks a defense claims to stop
 - JR Platt (“Strong inference”)

T4: Stop using the “Security is special” excuse

Claims that unique aspects of security exempt it from practices ubiquitous elsewhere in science are unhelpful and divert attention from identifying scientific approaches that advance security research.

But: intelligent adversaries, evolving technology, human factors ...

- astronomers: limited types of experiments
- disease scientists: exempt from scientific methods?



T5: Physics is not a role model for all of Science

*Physics-envy is counterproductive;
seeking “laws of cybersecurity” similar to physics
is likely to be a fruitless search.*

- *“most biology has little use for the concept of a law of Nature, but that does not make it less scientific”*

- P. Godfrey-Smith



T6: Crypto is not a role model for all of Security

*Crypto-envy is counterproductive;
many areas of security,
including those involving empirical research,
are less amenable to
formal treatment or mathematical role models.*

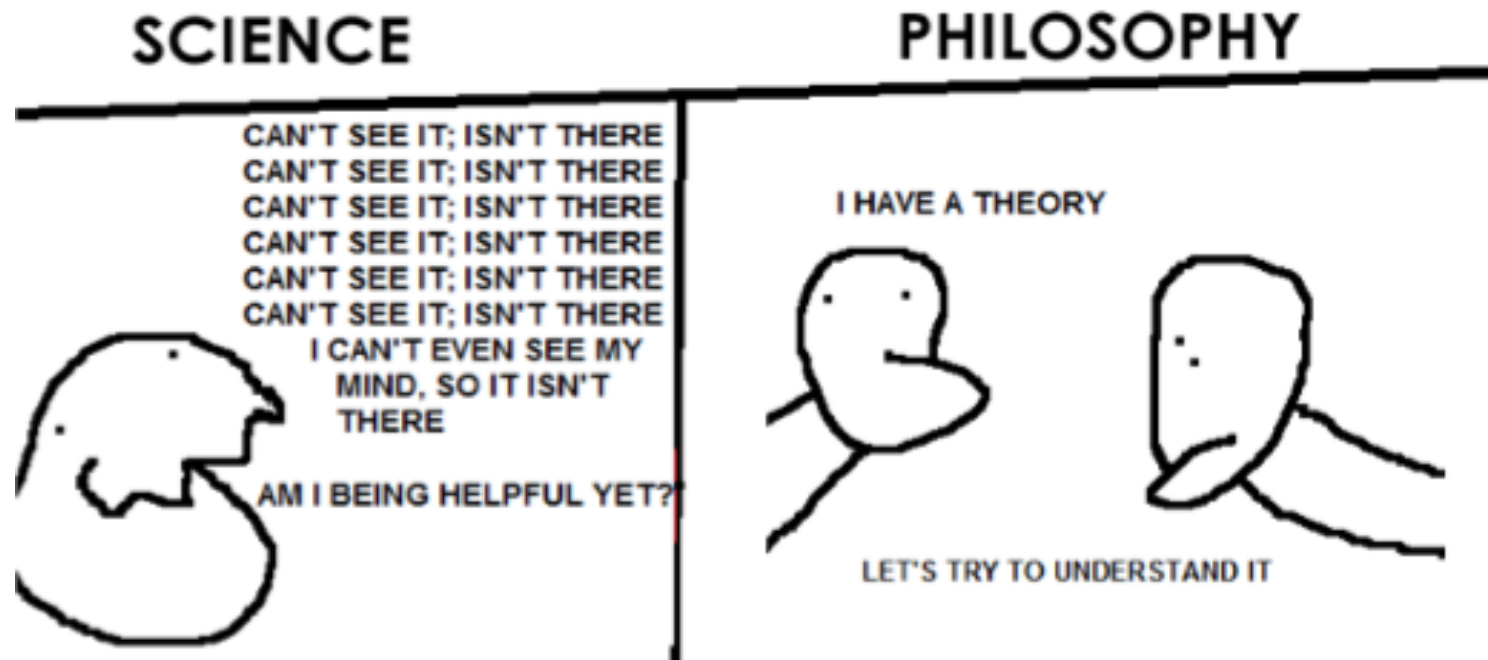


- “provable security” and misleading language
- *All models are wrong, some models are useful.* (G. Box)
- side-channel attacks



T7: Insist on bringing theory into contact with observation

*Both theory and measurement
are needed to make progress
across the diverse set of problems
in security research.*



T8: Insist results be put in context with full solutions

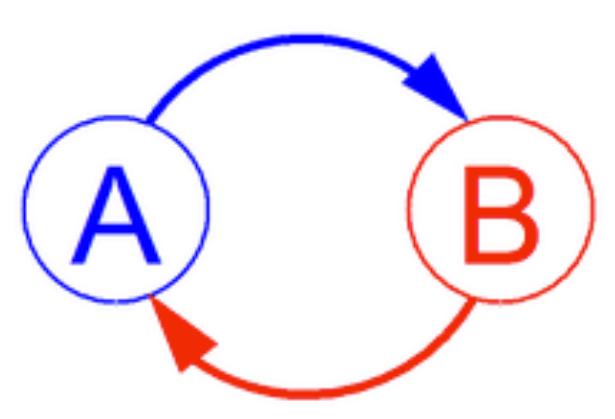
More security research of benefit to society may result if researchers give precise context on how their work fits into full solutions – to avoid naive claims of providing key components, while major gaps mean full-stack solutions never emerge.

- use-inspired basic research
(Stokes: *Pasteur's Quadrant*, 1997)



T9: Insist that assertions be supported by evidence

*Conflating
unsupported assertions & “argument-by-authority”,
with evidence-supported statements,
is an avoidable error
especially costly in security.*



T10: Insist on explicit claims and assumptions

*Despite consensus
that assumptions need be carefully detailed,
undocumented and implicit assumptions
are common in security research.*

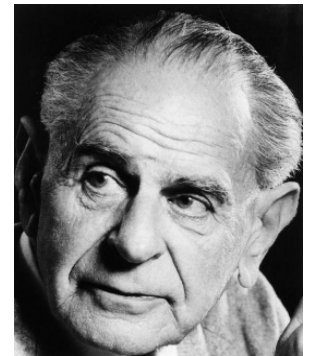
- “everyone understands these assumptions ...”
- *forcing function* to make assumptions explicit



T11: Insist on seeking refutation vs. confirmation only

*Science prioritizes efforts at refutation.
Empirical work that aims only to verify existing beliefs,
but suggests
neither new theory nor disambiguates possibilities
falls short of what science can deliver.*

*“If we are uncritical we shall always find what we want:
we shall look for, and find, confirmations, and we shall
look away from, and not see, whatever might be
dangerous to our pet theories” - Popper*



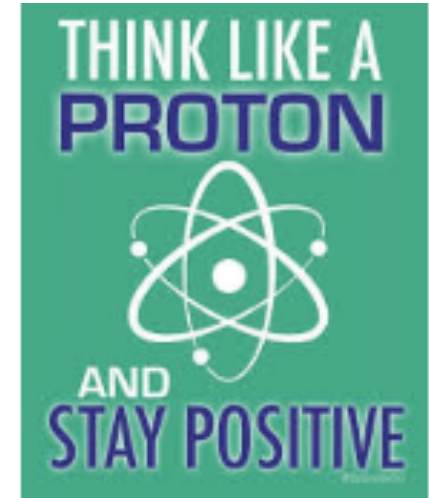
- Longstaff (ACSAC 2010), “Barriers to science in security”

Positive examples of scientific research in security

Password security

- Weir (CCS 2010)
- Zhang (CCS 2010)
- Bonneau (Oakland 2012)

- June 2017 rev of SP 800-63-3 (800-63B)
 - removed Appendix 1 (Jun 2004, “crude-entropy” reasoning)
 - now discourages: aging, complex pswd composition policies



Thank you ... Questions?

- references: Herley & van Oorschot (Oakland 2017; S&P mag 2018)

