SoK: Science, Security and the Elusive Goal of Security as Scientific Pursuit

Cormac Herley
Microsoft Research

P.C. van Oorschot
Carleton University

Need, Desire to do Security more Scientifically

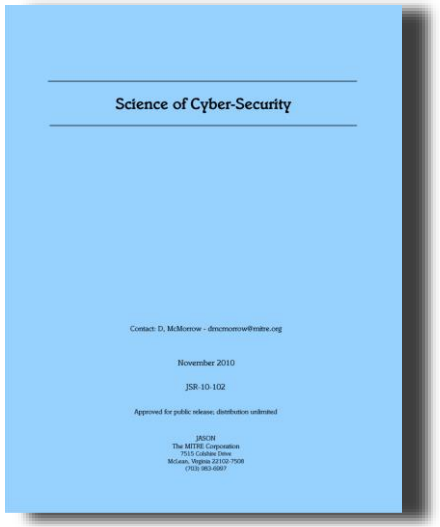
"Non-crypto security will remain a mess." A. Shamir.

"Pseudo-science and flying pigs" R. Schell.

NSA Science-of-Security program

SCIENCE OF SECURITY

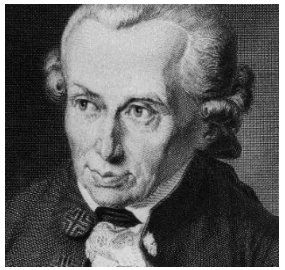
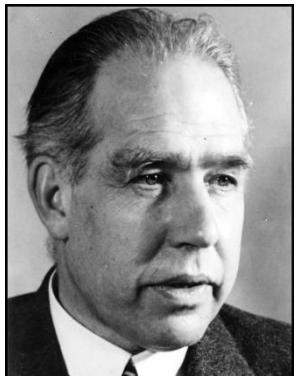
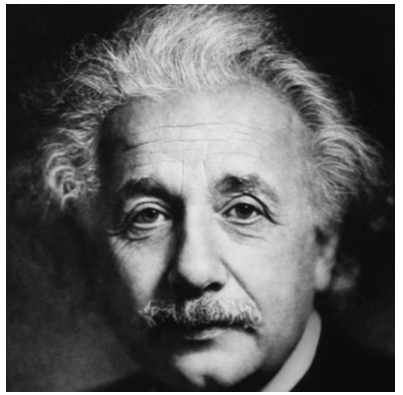
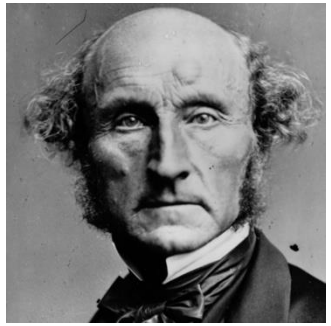
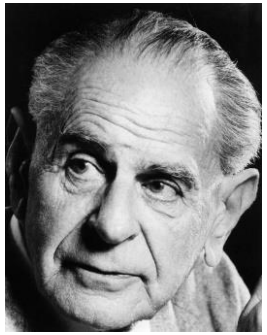
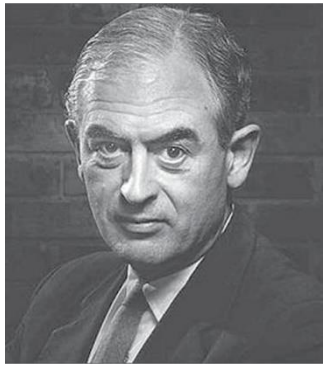
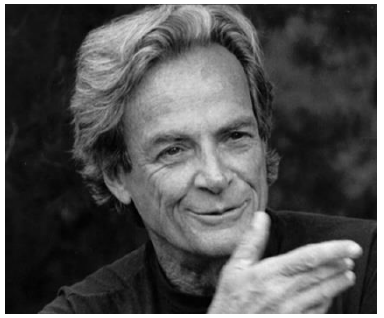
DoD JASON report



What do we mean by Science?

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

Philosophy/History of Science

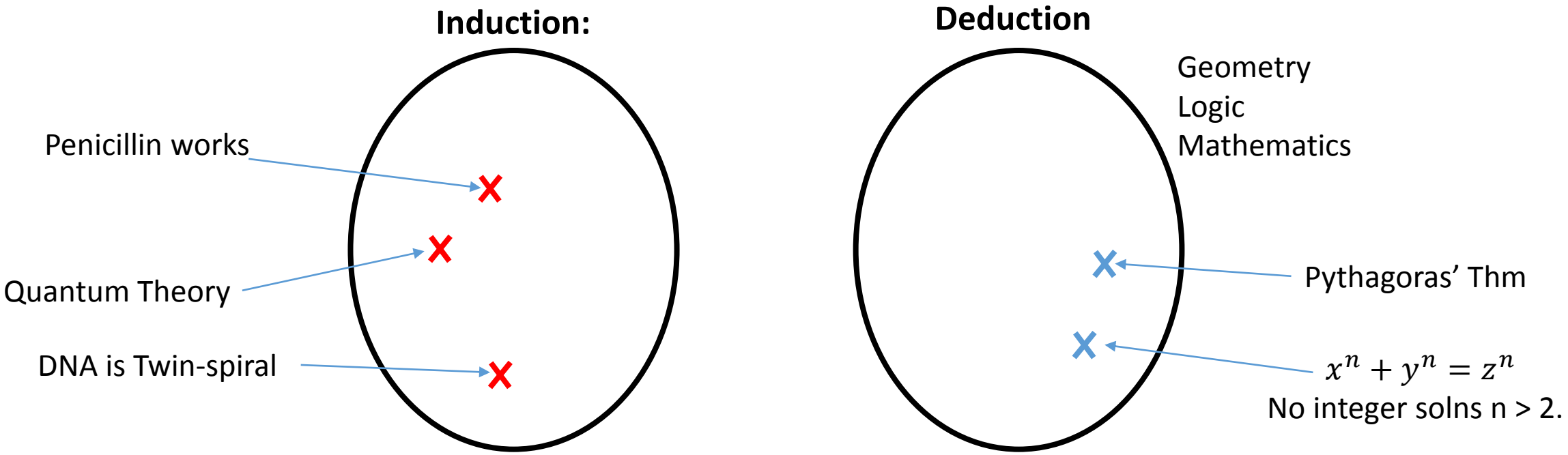
What's the consensus from other fields?

If theory conflicts with observation it's wrong.

Conflict with observation must be possible:

1. Science is induction not deduction
2. Claims must be falsifiable.

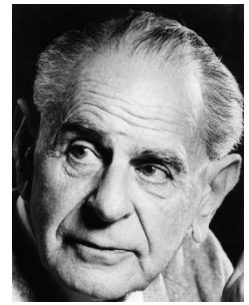
- **Induction:** statements about real world (always uncertain)
- **Deduction:** proved-true statements from axioms



	Inductive Statements	Deductive Statements
Describe real-world?	Yes	No

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



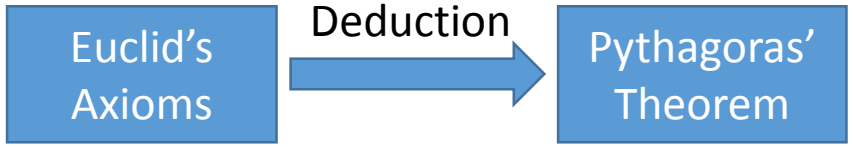
X cannot be falsified by any observation

$\Rightarrow$ X is consistent with every possible observation

$\Rightarrow$ Nothing observable depends on X

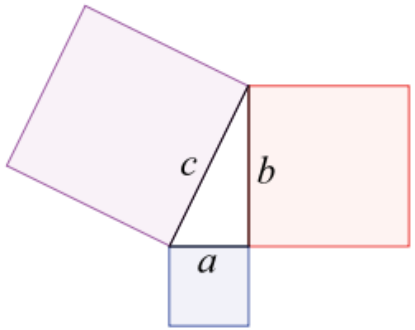
	Inductive Statements	Deductive Statements
Describe real-world?	Yes	No
Believe when:	Try to falsify and fail	Have a proof

Wait, Math isn't Science????



No observation contradicts Pythagoras' Theorem.

- If $a^2 + b^2 \neq c^2$ for the door we don't say theorem wrong.



Axiom: parallel lines meet at infinity

Assumption: attacker can't do log in a finite field

Observations contradicting assumptions are possible. Scientific claims retain uncertainty

Whether a real-world system satisfies assumptions is an empirical claim (and must be tested).

Reasonableness of assumptions is not a substitute for testing against observation

Newton: speed of fall ***in a vacuum*** $= g.t$

- Air pressure ≠ 0. We rely because predictions accurate.

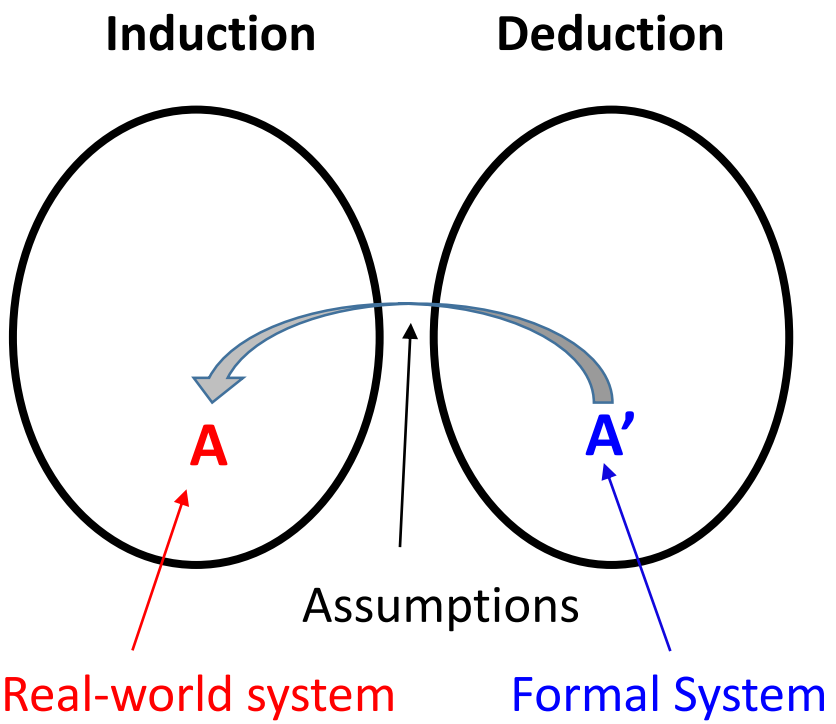
Reasonableness of assumptions is subjective

- Not an alternative to testing against observation
- Deduction:
  - Can reveal tautological consequences of assumptions
  - Cannot help determine if assumptions match reality

What does any of this have to do with security?

1. Failure to separate Induction/Deduction

Example Problematic Claim: *"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."*



Formal System A':

- Proof

Real-world System A:

- Proof + argument that assumptions match reality

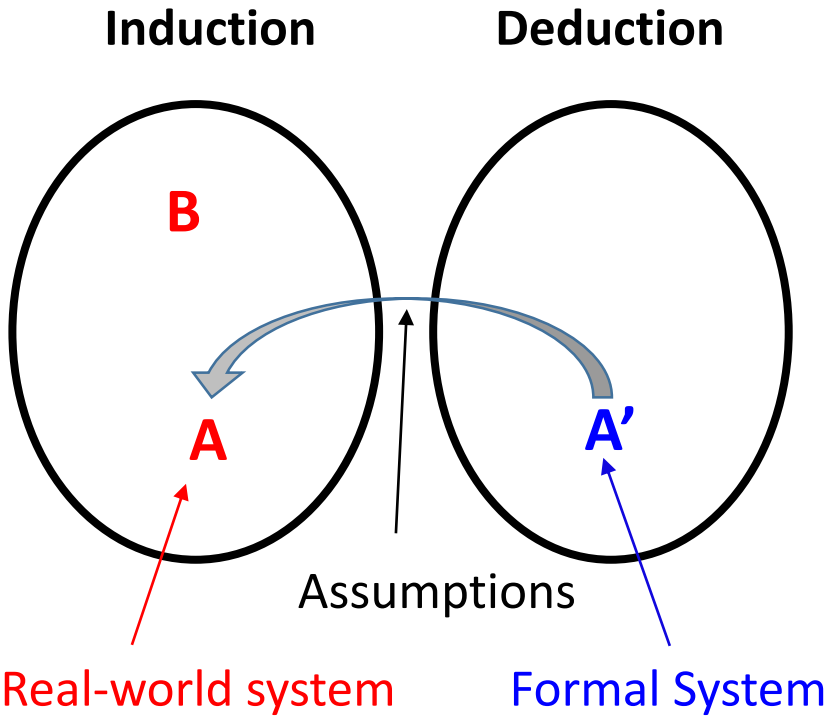
Whether assumptions match reality can only be explored empirically

1. Failure to separate Induction/Deduction

Example:

- **A':** attack on SSL 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
- No end-run around messiness of real-world



A proof + argument that assumptions are reasonable is not a proof. It's also not scientific w/o attempts to refute assumptions.

2. Failure to bring theory into contact with observation

"Passwords should contain a mix of upper, lower and special chars."
Morris&Thompson, 1979

Three+ decades of ***assuming*** this leads to more guess-resistant pwds.

What's the basis for claiming:

- *Passwords should be changed every 90 days.*
- *Should always obey browser warnings*

Do we have A/B tests? Observations of improved outcomes?

3. Reliance on implicit assumptions

Everyone agrees assumptions should be clearly stated

Precise list of assumptions for:

- Changing password every 90 days improves outcomes
- Choosing stronger passwords improves outcomes

Describe the evidence that would refute?

Hard to argue we've tried to falsify assumptions we can't list!

Reliance on Unfalsifiable Claims

Can't observe that real-world system is secure.

$\Rightarrow$ Claim that real-world system is insecure unfalsifiable

(would require observing that it is secure)

$\Rightarrow$ Claims of necessary conditions for real-world security unfalsifiable.

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

- E.g., Choose a password that withstands 10^{14} guesses

Conclusions:

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

- Simply announcing a desire for more Science is empty
- Exhortations to be more scientific are circular
- Valuable lessons ignored

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

- Every scientific statement contains uncertainty
- Assumptions must be subjected to refutation
- This comes up over and over

Claims that unique aspects of security exempt it from a scientific approach are unhelpful.

- "But active adversary, no fundamental laws, man-made artifacts….."
- Science isn't applicable only in rare circumstances
- Science is just the best way we know of making inferences
  - Self-correction, acknowledgment of fallibility