



UNIVERSITÄT **BONN**

Make Security Scientific Again

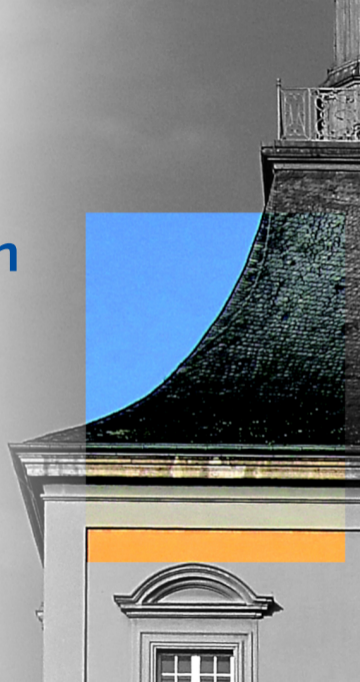
How scientific is our work?

Ben Swierzy, Timo Pohl

{swierzy,pohl}@cs.uni-bonn.de

University of Bonn | Institute of Computer Science 4

Oberseminar | Bonn | 17.04.2025



2017 IEEE Symposium on Security and Privacy

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

Cormac Herley
Microsoft Research, Redmond, WA, USA
cormac@microsoft.com

P.C. van Oorschot
Carleton University, Ottawa, ON, Canada
paulv@scs.carleton.ca

Abstract—The past ten years has seen increasing calls to make security research more “scientific”. On the surface, most agree that this is desirable, given universal recognition of “science” as a positive force. However, we find that there is little clarity on what “scientific” means in the context of computer security research, or consensus on what a “Science of Security” should look like. We selectively review work in the history and philosophy of science and more recent work under the label “Science of Security”. We explore what has been done under the theme of relating science and security, put this in context with historical science, and offer observations and insights we hope may motivate further exploration and guidance. Among our findings are that practices on which the rest of science has reached consensus appear little used or recognized in security, and a pattern of methodological errors continues unaddressed.

Index Terms—security research; science of security; history of science; philosophy of science; connections between research and observable world.

I. INTRODUCTION AND OVERVIEW

Security is often said to have unique challenges. Progress can be harder to measure than in areas where, e.g., perfor-

research) in the light of consensus views of science and scientific methods. We find that aspects from the philosophy of science on which most other communities have reached consensus appear surprisingly little used in security, including in work done under the SoS label. For example, we do not find that that work better adheres to scientific principles than other security research in any readily identifiable way.

We identify several opportunities that may help drive security research forward in a more scientific fashion, and on this we are cautiously optimistic. While we see great benefit to this, we also do not wish to argue that all of security must be done on rigidly scientific principles. A significant component of security is engineering; this shares with science the regular contact with, and feedback from, observation, despite not having as clearly articulated a definition or methods.

Section II selectively reviews literature on the history and philosophy of science, with particular emphasis on three things: 1) methodologies and positions on which practicing scientists and philosophers of science have largely reached consensus; 2) aspects highlighting opportunities to eliminate

What is Science?

Inductive and Deductive Statements

Inductive Statements: After many observations we infer rules for things not yet observed.

Deductive Statements: Theorems follows with certainty from a self-consistent set of axioms.

Inductive and Deductive Statements

INDUCTIVE

DEDUCTIVE

Inductive and Deductive Statements

INDUCTIVE

All swans are white

DEDUCTIVE

Inductive and Deductive Statements

INDUCTIVE

All swans are white

Proof by induction

DEDUCTIVE

Inductive and Deductive Statements

INDUCTIVE

All swans are white

Proof by induction

The PC is secure

DEDUCTIVE

Inductive and Deductive Statements

INDUCTIVE

All swans are white

Proof by induction

The PC is secure

AES-256 is more secure than AES-128

DEDUCTIVE

Science progresses by finding errors

Falsification



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

K. Popper (1959)

” As far as the laws of Mathematics refer to reality they are not certain, and as far as they are certain they do not refer to reality. “

A. Einstein

Hypothetico-Deductive Model

Foundational Properties:

Consistency, Falsifiability, Predictive power and progress

Basic Scientific Method

- 1 Form hypotheses from observations
- 2 Formulate falsifiable predictions (*models*) from those
- 3 New observations can either support or reject these

Interlude: Approaching Science of Security

Claims On What Security Research Needs

” By its very nature, there [...] cannot be empirical evidence for the security of a design. “

H. Krawczyk, 2007

Example:

Usable Security has shown that actual user behavior deviates enormously from what was modelled or assumed



” stop insisting that quantitative is better than qualitative; both types of measurement are useful “

S.L. Pfleeger, 2007

” Little evidence supports the hypothesis “security can correctly be represented with quantitative information” “

V. Verendel, 2009

Typical security researcher study programs offer little training in experimental science or scientific methods.

Class *Vulnerability Papers*

shows that a software can be exploited

(unscientific)

Class *Attack Methodology Papers*

presents a new class of attacks

(scientific)

Is Security Special?

Adaptive Adversary



Absence of Invariant Laws

Example: Physics

- universal laws
- continuous refinement and extensions of theories

Security is too intertwined with human behavior to have similar laws and models.

Man-Made Artifacts

- Artificially constructed environment
- Weakly tied to the physical universe
- Constantly and rapidly evolving conditions

Against This View

- Philosophy of Science is independent of preconditions

Against This View

- Philosophy of Science is independent of preconditions
- Disregarding Science implies disregarding the need for its basic properties

Against This View

- Philosophy of Science is independent of preconditions
- Disregarding Science implies disregarding the need for its basic properties
- Pleading uniqueness to avoid being held to scientific approaches is common in unscientific fields

Failures in Security Research

Examples

- Provable Security
- A 128-bit key is more secure than a 64-bit key
- A system protected by a password is more secure than one without

Possible Structure of Claims:

- In order to be secure you must do X
- X improves security

Example:

- A password must have at least 8 characters and contain letters, digits and special characters to be secure

Failure to Make Claims and Assumptions Explicit

Examples

- User Training is inherently beneficial.
- Users should be pushed to use 2FA.

Failure to Seek Refutation rather than Confirmation

Much empirical work in security

- neither generalizes to suggest a new hypothesis
- nor presents a severe test to an existing one

Failure to Seek Refutation rather than Confirmation

Much empirical work in security

- neither generalizes to suggest a new hypothesis
- nor presents a severe test to an existing one

Examples

- Attack Papers
- Null Hypothesis Significance Testing
- Mechanical Turk

Ways Forward

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

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

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.

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

Science prioritizes efforts at refutation. Empirical work that aims only to verify existing beliefs, but does not suggest new theory or disambiguate possibilities falls short of what science can deliver.

Takeaways

Your work is likely scientific if

- challenges existing assumptions or
- proposes a model.

Models are judged by their predictions.

State your claims precisely. Vague formulations are rarely wrong but do not provide much value.

DISCUSSION