3 dubious concepts in Science of Security

Dusko Pavlovic

Royal Holloway

Washington DC
November 2012

Outline

Nature

Method

Law

Outline

Nature

Method

Law

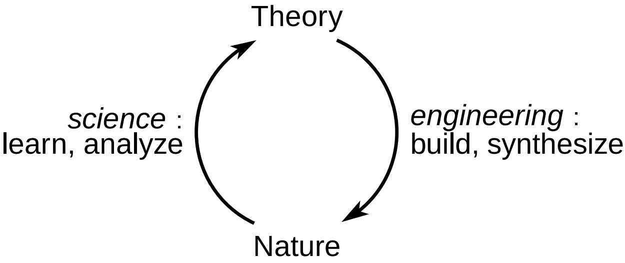
Background: Science *vs.* Engineering

It is the aim of the natural scientist to discover mathematical theories, formally expressed as predicates describing the relevant observations that can be made of some physical system. [. . .]

The aim of an engineer is complementary to that of the scientist. He starts with a specification, formally expressible as a predicate describing the desired observable behaviour of a system or product not yet in existence. Then [. . .] he must design and construct a product that meets that specification.

Tony Hoare
Programs are predicates

Background: Science *vs.* Engineering



Theory

science :
learn, analyze

engineering :
build, synthesize

Nature

Thesis 1

Security is (mostly) Engineering

- Science is concerned with natural phenomena.
- Security is a property of artifacts (software . . .).
- Symbolic artifacts are not natural phenomena.
- Therefore security is not a subject for science.

Antithesis 1

Symbolic artifacts can be natural phenomena

- The fact that a car is an artifact does not mean that its behavior is not a natural process.
  - But car is a physical object. Software is not.

Antithesis 1

Symbolic artifacts can be natural phenomena

- The fact that a car is an artifact does not mean that its behavior is not a natural process.
  - But car is a physical object. Software is not.
- The fact that a gene does not have a mass does not mean that a gene is not a natural phenomenon.
  - A gene can be separated from the chromosome / chormoneme, and, e.g., published in a paper.

Antithesis 1

Symbolic artifacts can be natural phenomena

- The fact that a car is an artifact does not mean that its behavior is not a natural process.
  - But car is a physical object. Software is not.
- The fact that a gene does not have a mass does not mean that a gene is not a natural phenomenon.
  - A gene can be separated from the chromosome / chormoneme, and, e.g., published in a paper.
- The fact that software is an artifact with no mass does not mean that computation is not a natural process.
  - The Web is a software system. Its computation is a natural process.

Antithesis 1

Computation is a natural process

- Landauer: Information is physical
- Bennett: Evolution is a computational process

Antithesis 1

Cyberspace is a part of Nature

- Landauer: Information is physical
- Bennett: Evolution is a computational process
- Network-as-computer is an evolutionary system
    - It originated as an engineering artifact.
    - It evolved into a carrier of natural processes.
    - **Hence cyber security problems.**

Outline

Nature

Method

Law

Thesis 2

Science of Security = Science + Security

- Science is the method to systematically understand the observed phenomena and predict future behaviors.
  - Scientific method was *invented* (by F. Bacon et al.)

- Security practices lack a method to systematically understand security problems and predict the future behaviors.
  - We need to *invent* a Science of Security
    - combine various sciences into a new one
    - add the experimental method to CS

Antithesis 2

Science was not invented, but discovered

- Science was already there.
  - It evolves as a natural way to interact with nature.

Antithesis 2

Science was not invented, but discovered

- Science was already there.
    - It evolves as a natural way to interact with nature.
- Science of security is already there ($\leftsquigarrow$ F. Schneider)
    - We need to *uncover* scientific theories and **laws** of security within the existing work, and start from there.

Outline

Nature

Method

Law

Background: Motivations for SoS

Requirement

- Security methods should be precise and systematic.
- Not ad hoc, not an art or a craft.

Background: Motivations for SoS

Idea

- Formal methods made security more precise
  - making and checking formal models

- But formal methods lack a process for aligning theories with the world
  - measurable validation
  - experimental method

- Science is the process for aligning theories with the world
  - We need Science of Security

Background: Motivations for SoS

Idea

- Formal methods made security more precise
  - making and checking formal models
- But formal methods lack a process for aligning theories with the world
  - measurable validation
  - experimental method
- Science is the process for aligning theories with the world
  - We need Science of Security
  - We seek **persistent laws of security**.

Thesis 3

Science provides persistent laws.

Thesis 3

For the mathematician there is no Ignorabimus, and, in my opinion, not at all for natural science either... The true reason why [no one] has succeeded in finding an unsolvable problem is, in my opinion, that there is no unsolvable problem.

In contrast to the foolish Ignorabimus, our credo avers:

We must know, We shall know!

David Hilbert

Königsberg Address (September 8, 1930)

Antithesis 3

Every law of physics is wrong in some ultimate detail, although some are awfully good approximations. But none is absolutely valid.

John Tukey

Process of Science

If we have a definite theory, from which we can compute the consequences which can be compared with experiment, then in principle we can prove that theory wrong.

Process of Science

. . . *But notice that we can never prove it right.*

Suppose that you invent a theory, calculate the consequences, and discover every time that the consequences agree with the experiment. The theory is then right? No, it is simply not proved wrong. In the future you could compute a wider range of consequences, there could be a wider range of experiments, and you might then discover that the thing is wrong.

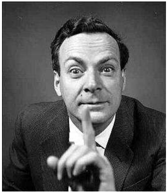
Process of Science

That is why laws like Newton's laws for motion of planets last such a long time. He guessed the law of gravitation, and it took several hundred years before the slight error in the motion of Mercury was observed. During all that time, the theory had not been proven wrong, and could be taken temporarily to be right.

Process of Science

We never are definitely right;
we can only be sure when we are wrong.

Richard Feynman
Lectures on the Character of Physical Law



The best kept secret of Science

- Science does not provide persistent laws
- Science only provides methods to improve theories

Religion, Art, and Science

Religion says: This is the truth about the world.

- You can rely upon it.

Religion, Art, and Science

Religion says: This is the truth about the world.

- You can rely upon it.

Art says: This is a story about the world.

- You can relax and play with it.

Religion, Art, and Science

Religion says: This is the truth about the world.

- You can rely upon it.

Art says: This is a story about the world.

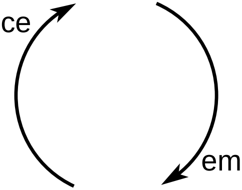
- You can relax and play with it.

Science says: This a theory about the world.

- You shouldn't rely upon it too much.
- You shouldn't relax, but work to improve it.

Upshot

Process of Science


Theory

inductive inference

empiric testing

Counter-evidence

Science never settles on a theory.
It loops through counter-evidence forever.

Richard Feynman on Science of Security

If we have a precisely defined security claim about a system, from which we can derive the consequences which can be tested, then in principle we can prove that the system is insecure.

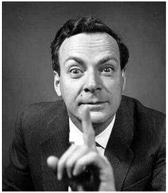
Richard Feynman on Science of Security

. . . But we can never prove that it is secure.

Suppose that you design a system, calculate some security claims, and discover every time that the system remains secure under all tests. The system is then secure? No, it is simply not proved insecure. In the future you could refine the security model, there could be a wider range of tests and attacks, and you might then discover that the thing is insecure.

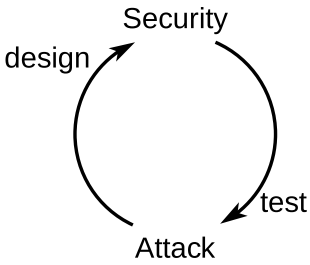
Richard Feynman on Science of Security

We never are definitely secure;
we can only be sure when we are insecure.



Upshot

Process of Science of Security



Security never settles on a claim.
Every security claim has a lifetime.