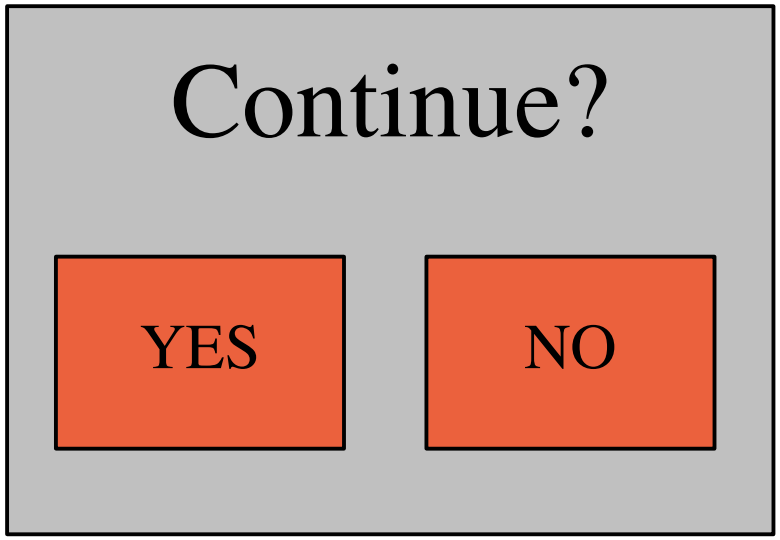
The need for and progress in science for information protection and digital forensics

IEEE Oakland Conference – May 25, 2011

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- The future



Your speaker

- CEO - Fred Cohen & Associates / President CalSci
  - Enterprise information protection architecture
  - Digital forensics for (usually high-valued) legal cases
  - 501(c)3 research and educational institution
  - M.S. Advanced Investigation / Ph.D. Digital Forensics
- B.S. EE (C-MU '77), M.S. Info Sci (Pitt '81), Ph.D. EE (USC '86)
- >30 years of information protection R&D, design, engineering, testing, implementation, operation, etc.
- >20 years since first digital forensics case
- POST certified instructor in digital forensics, Guest lecturer FLETC, PMTS Sandia National Labs, etc.
- >>100 peer reviewed publications, many conference talks, …

The basics

- Science is about causality
  - A scientific theory:
    - C $\rightarrow^{M}$ E: Cause(C) produces Effect (E) via mechanism M
- The scientific method
  - Identifies the criteria for rejecting (or accepting, for now) a scientific theory
    - Hypothesize C $\rightarrow^{M}$ E
    - Perform experiments to refute
    - Failure to refute → confirmation
    - Enough confirmations and hypothesis becomes theory
    - One refutation and theory becomes refuted (wrong)
      - But it may still be useful for limited cases

Example science

- Hypothesis: The World is flat
- Experiment: Keep sailing West
  - See if you come back from the East
  - Lots of them didn't come back… confirmed
  - So many didn't come back → scientific theory
  - One made it around…
- Refutation – the theory was refuted (wrong)
  - But it may still be useful for limited cases
    - Do you account for the curvature of the Earth when you design a building?
    - Or do you assume the Earth is flat?

A problem with science

- Scientists are people too
  - People make mistakes → Science makes mistakes
  - Science corrects big mistakes and does it slowly
    - When someone notices “something wrong”
    - When the wrong thing is important enough to someone
    - Scientists will check it out, refute the old, propose new
    - Old workable science is still useful (F=ma)
  - People lie → science examines refutation carefully
    - Confirmation not so much – because it's not surprising
    - A new result that's important will get checked out
    - Once you lie in science - nobody will likely believe you again – and your old work will be largely discounted

Science (protection & forensics)

- Is digital forensics important enough to care?
  - It sends people to jail / kills / frees them
  - It forms a framework for the legitimacy of the courts – and civil society
  - The social contract fails if science does not aide justice
- Is information protection important enough?
  - We have created a highly dependent society
  - Advanced society may literally collapse without properly functioning information technology
- I think it's important enough, so I care... do you?

But suppose we don't care?

- Without a reliable C $\rightarrow^{m}$ E model
  - We make a lot of mistakes (which happens anyway)
  - Those mistakes don't get corrected
  - They may be replaced by other mistakes
- How's that working out for you?
  - We pay too much and get too little
  - Snake oil sales prosper in the marketplace
  - We still do ridiculous things we did 25 years ago
    - Change your password how often?
- A scientific approach may help us get to “right”

The draft NITRD issue

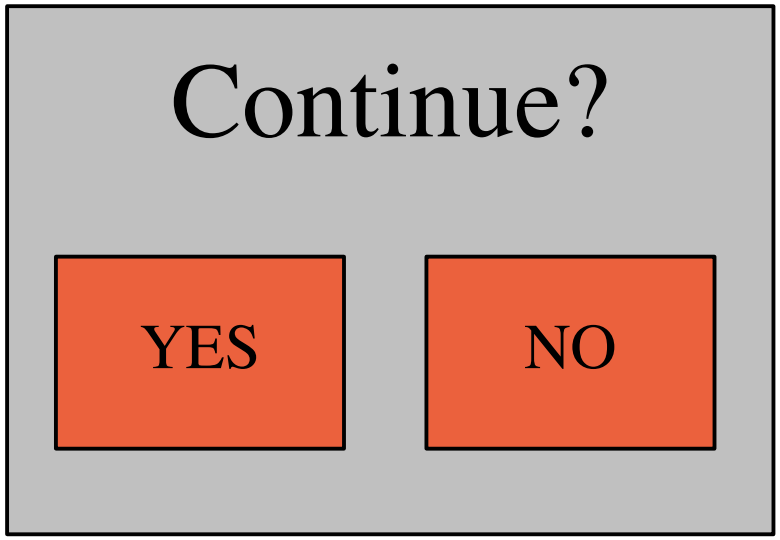
- 10-year effort
- Develop an organized, cohesive foundation to the body of knowledge – a rigorous scientific foundation to cybersecurity
  - Organize disparate areas of knowledge
  - Discover universal laws
  - Apply the rigor of the scientific method
  - Predictive, explanatory, general purpose laws
  - Scientific bases for engineered cybersecurity solutions

The list of stuff

- Methods to model adversaries
- Component, policy, and system composition
- Control theory for maintaining security in the presence of partially successful attacks
- Sound methods for ~~integrating humans in the system~~: usability and security
- Quantifiable, forward-looking security metrics ~~(using formal and stochastic modeling methods)~~
- Measurement methodologies and test beds for security properties
- Comprehensive, open, and anonymized data repositories

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- The future



Some simple questions

- What is the definition of risk?
  - What are its units?
  - What is the standard of measurement?
  - Is it an absolute quantity?
- What can we do to it?
  - Transfer: Is there any benefit to the shell game?
  - Reduction: By how much and with what method?
  - Avoidance: What are the units of reward?
  - Acceptance: Only if we know what it is…
  - ARE THOSE THE ONLY THINGS TO DO?

Consensus: Digital Forensics

- The “scientific community” in digital forensics lacks consensus even around the very basic notions
- Compared to the consensus on human activity producing global climate change (86% or more) the basic notions of digital forensics are not at consensus levels:
  - Digital evidence is made of bit sequences.
  - You can observe bits without altering them.
  - You can duplicate bits without removing them.
  - Digital evidence is trace evidence

Challenge!!!

- There are only about 500 peer reviewed articles on digital forensics in the literature
  - Terminology is not widely agreed or uniformly applied – lots "made up"
  - Testability, validation, and scientific principles have not been widely addressed
  - The small corpus of published results limits the scientific basis for statements
  - Claims w/out supporting experiments common.
- "The State of the Science of Digital Evidence Examination" - 2011 IFIP DF conference

Consensus: Info. Protection

- We have some reasonably consistent words
  - Most CISSPs use many of the same words
    - Although they don't mean exactly the same things
  - There are 10,000+ peer reviewed articles
    - ~5 real journals (outside of cryptography)
    - Scores of peer reviewed conferences
  - Testability, validation, and scientific principles have not been widely addressed
  - Claims w/out supporting experiments common
  - Lots of long-term mistakes and rote approaches
  - Words are not consistently enforced in publications
  - No standard wordings (like there are in psychology)

Info Pro Big Problems

- There are almost no scientific experiments
  - No widely used theory of measurement
  - Almost no useful metrics
    - Progress in the attack graph with time (units?)
  - Almost no scientifically valid experiments
  - We don't even have a physics...
- A big part of the problem:
  - We have a purely mathematical basis
  - It ignores the people and processes
- A big part of the solution:
  - Social sciences integrated with artificial sciences

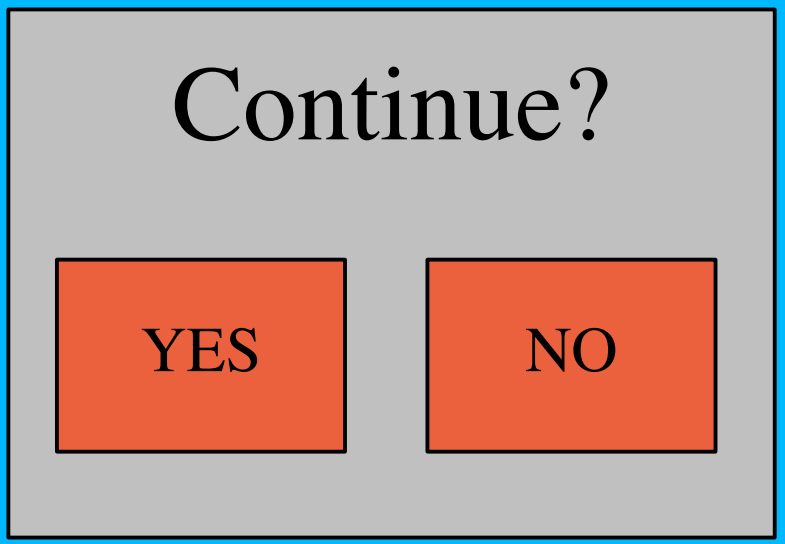
Another social problem

- Science is about refutation
  - When you say something, expect a challenge
    - On a rational and relevant basis
  - If you can't answer the challenge, you're refuted
    - Sort of – for now...
- But decision-makers in this space don't like it
  - Example: risk aggregation in large-scale systems
  - Example: computer viruses vs. trusted systems
  - Example: security theater vs. measurable basis
- We could use some executives who seek refutation rather than "yes – you're right"

And another critical issue

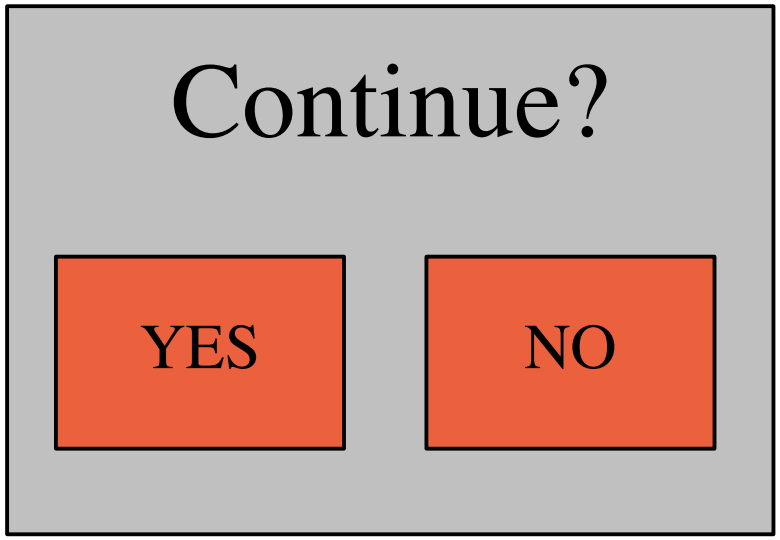
- Information protection involves people
  - As a field we don't seem to apply the human research areas to our work very often or well
    - Sociology, psychology, social psychology, etc.
    - Behavioral models and cognitive limitations
    - Decision-making methodologies and metrics
  - Without addressing the human aspects, we are destined to fail to meet our protection objectives
- A saying of mine
  - The “hard” sciences are the easy sciences
  - The “soft” sciences are the hard sciences

The file you downloaded is from an untrusted source. Since we cannot verify the source of this file, it may contain any of a wide range of different security implications that cannot be determined in advance with current technology. Please either (1) contact your security officer or SPO office prior to using the program, (2) make an independent determination that this file is what was desired or not, and based on that determination make a prudent decision about its use, or (3) review the detailed security documentation on file at the SPO file folder on your enterprise desktop helpdesk recall page.

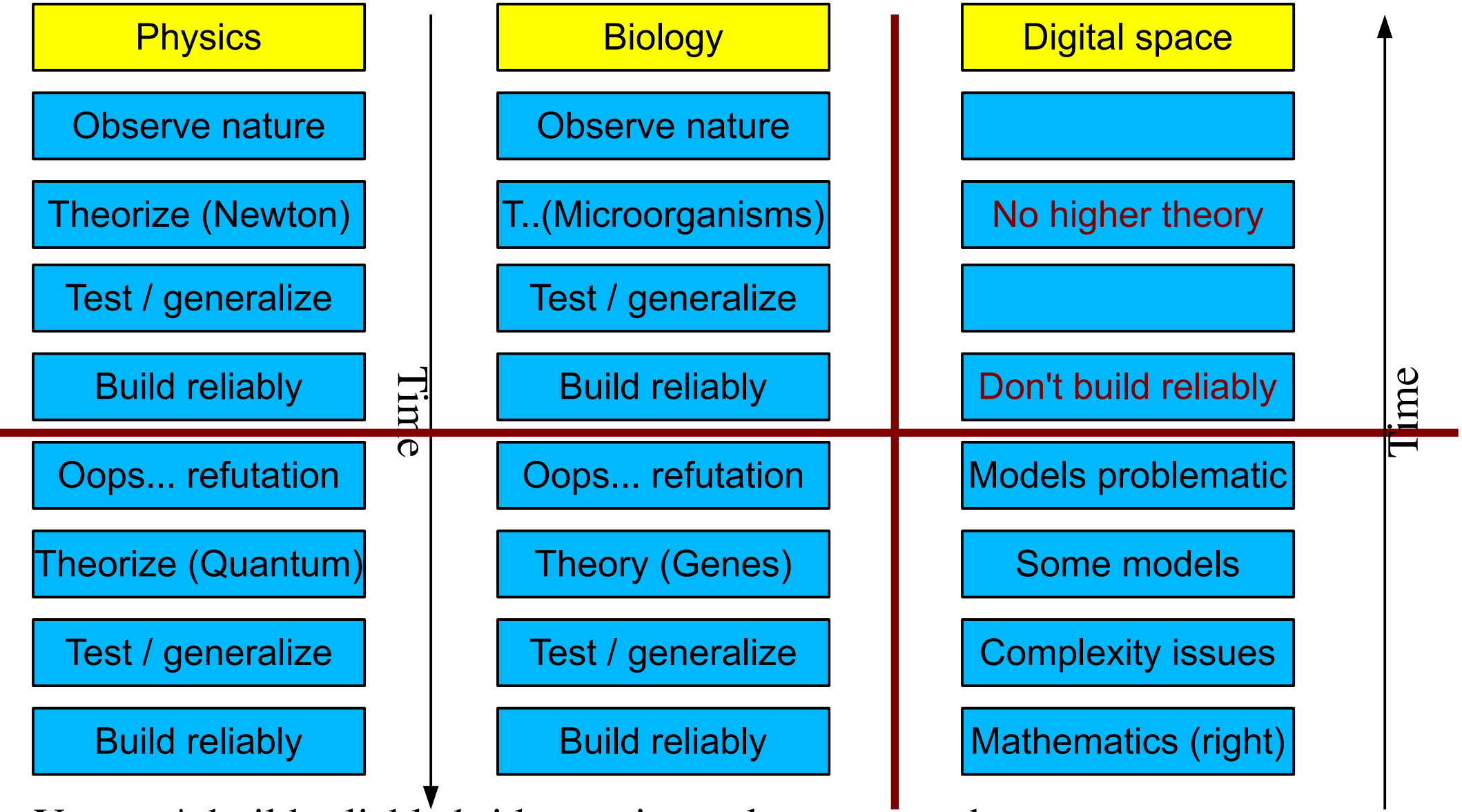


Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- The future



How did some sciences form?



You can't build reliable bridges using only quantum theory
You can't reliably cure diseases using only genetic theory

Approaches to protection science

- Mathematics
  - Keep building from the bottom
  - Hope to construct our way out of it
  - Complexity issues
- Archeology
  - NSF approach to DF
  - Requires a physics
  - Problematic for reliable results
- Engineering
  - Build and test
  - Find and fix
  - Requires a physics
  - Bridges are falling
- Social sciences
  - Statistics: Causality is too complex / unknown
    - P(x) problematic
    - Measure what? How?

Notions of a new approach

- Information physics
  - We may want a "physics of digital information" level to reduce complexity and allow composition based on physics properties
- Social sciences
  - We may want a "behavioral science" area to address the human and social factors associated with protection
- Fusion (***IRB decision is involved***)
  - Example: Deception experiments from ~2000
  - Human and group dynamics taken into account
  - Measured progress in attack graphs with time
  - Differential effects of 3 types of "deceptions"

Transfer vs. Trace

- **Natural world** forensics
  - **Transfer** is the scientific basis for trace evidence
  - When physical objects come into contact, each leaves part of itself with the other(s) (Locard misquote)
    - Scientific theory: Objects: Contact $\rightarrow^{\text{Transfer}}$ Traces
  - Traces found on objects are consistent with transfer from physical contact with other objects
- There is **no transfer in digital evidence**:
  - The **scientific basis** for evidence acceptance in the **natural world does not apply**
- But there are still **traces** (product of execution)
  - Scientific theory: FSM $\rightarrow^{\text{Execute}}$ Traces

A different physics?

- Some basic physics of the digital world:
  - **Digital data** is entirely **sequences of bits**
  - The atomic unit is the "bit"
  - Nothing smaller (finite granularity)
    - No longer dealing with the digital evidence
    - Smaller than a bit it's physical evidence
  - Finite bit granularity → finite time granularity
    - Bits can only store traces (of time) at finite granularity (a finite bit sequence)
- **Normal space: infinite** granularity space/time
- **Digital space: finite** granularity space/time

Finite granularity issues

- Finite granularity → time is a partial ordering
  - A before B (A<B), A after B (A>B), Can't tell (A≈B)
  - Traces as recorded are subject to Δt
    - What is the Δt for your traces / time stamps?
  - Is the claim a sequence of events?
    - Don't know Δt → don't know the sequence!
- Precision vs. accuracy
  - Trace time stamps are subject to delays, etc.
    - They look precise (2010-11-02 03:34:54.455)
    - But often aren't as accurate (off by 9 hours)
  - Mixed granularity misleading as to sequences
    - Some Windows time stamps at 1-day granularity

Convergence vs. divergence

- FSMs have "perfect" forward predictability
  - Given an FSM, initial state, and input sequence, all state and output sequences are precisely defined
  - Many FSMs and input sequences produce identical output sequences
  - **Digital space "converges" with time**
    - Traces do not uniquely identify causes!
    - $C \rightarrow^{m} E \not\Rightarrow E \rightarrow C$ – **Effect does not imply (unique) cause!**
- **Normal space** (physics) admits to only one past but many possible futures: E→C unique!!!
  - **Normal space "diverges" with time!**
    - **Effect implies unique cause**

Convergence details…

- Digital space converges with time
  - FSM: (I,O,S,m:{IxS}→{O,S'}) IF |I|>(|O|+|S|) THEN ∃(i,i')∈I:∃(o)∈O,∃(s)∈S, i→(o,s) and i'→(o,s)
  - Also note that $h(O) \leq h(I+S)$ (Shannon's *h*)
  - **Normal space diverges with time** *(2nd law of thermodynamics)*
  - **Digital space converges with time**
- You can't normally identify I^n from traces T
  - T: $|T|<|I^n|$, $\exists(i,i')\in I^n:\exists(t)\in T$, i→(t) and i'→(t)
  - In digital space, history is not uniquely determined by the present

Latent nature and tools

- Bits (and DFE) are (normally) latent in nature
  - Bits can't be directly observed with human senses
    - The bits must be observed through tools
  - How do we understand and trust the tools?
    - Most tools are computer programs (sequences of bits interpreted by FSMs)
    - How do we assess and present tool reliability?
  - A scientific methodology to evaluate tools?
    - No methodology → regardless of what the tools tell us, we don't know how to interpret it
    - What is the basis for trusting your tools?
    - In most cases, no basis is provided
    - Do you know the scientific principals and methods?

How do we know?

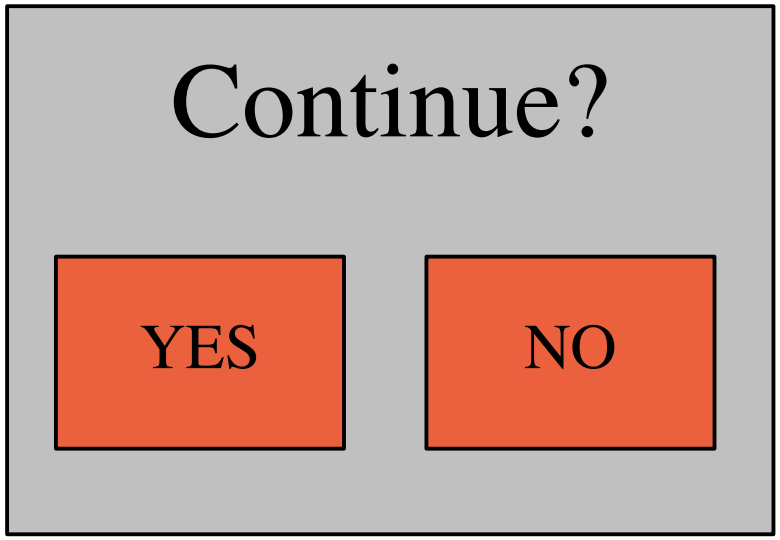
- How do we calibrate and test tools?
  - Calibration → validation with known samples
    - What known samples are right for the matter?
    - What is the "right" answer and how do we tell?
  - Testing involves software verification
    - Mathematical proofs
    - Tests against error models
  - A theory of measurement is needed:
    - What does the tool measure? How does it do it?
    - Do I need / can I use the same tool to test it?
    - Can I use a tool that doesn't reveal mechanisms producing its outputs?

Differences in physics …

- There are many more examples of differences between the physics of digital information and the physics of the natural world.
- For details see:
  - F. Cohen, "Digital Forensic Evidence Examination - 3rd ed.", ASP Press, 2011

Outline

- Introduction – the basics and the need
- Science as a social activity
- A different physics – an attempt at a theory
- The future



An engineering discipline

- An approach to building reliable protection
  - A science base that produces methodologies, scientific theories along with limitations, measurement methods, defined language and usage, and experimental basis for showing properties of components and composites.
  - A set of well tested tools and techniques for analysis and construction of mechanisms with known properties and identified limitations not requiring expertise in the lowest level of minutia.
  - A global feedback mechanism for improvement over time, including a rich set of peer reviewed publications, professional standards, and strong educational base with common real knowledge

Where from here?

- The social part of science...
  - Here I am – trying to convince you
    - If I do, you will try to convince others
  - In the marketplace of ideas, mindshare wins
    - For a while... until failures force abandonment
    - Refutation is king
  - The "meme"s that survive are more "fit"
    - In the environmental niches they live in
  - Evolution is not optimization
    - But refutation pushes us out of our gravity wells
- I would love to discuss your research...

Thank You

http://calsci.org/ - calsci at calsci.org
http://all.net/ - fc at all.net