# The need for science and engineering disciplines to move the information protection field forward

CMU-CyLab – 2013-02-11

Dr. Fred Cohen
CEO – Management Analytics
CEO – Fred Cohen & Associates

# Outline

- My background
- Measurement and Science
- The human reality of science and protection
- The physics of digital information
- The future

**Abstract:**

Science and engineering develop with the introduction of systematic approaches to understanding reality.

Information protection, a mix of the easy things (called the hard sciences), and the hard things (called the soft sciences).

Ultimately an information physics is needed

Historical lines fused across disciplines

# Your speaker

- CEO – Management Analytics / Fred Cohen & Associates
  - Protection architecture / Counsel to executives
  - Tool development / Patents / Basic research (R1)
  - Digital forensics for (usually high-valued) legal cases
  - Government sponsored research and development (R2-3)
- 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 DF instructor, Guest lecturer FLETC, PMTS Sandia National Labs, ICS$^2$ fellow, honorary Ph.D. in C.S., etc.
- >>100 peer reviewed publications, many conference talks, …

**Summary: He's old... and getting older...**

# Outline

- My background
- Measurement and science
- The human reality of science and protection
- The physics of digital information
- The future

# When I was young...

- 1973 – CMU undergrad – soon to be E.E.
- Dr. B. R. Teare – University professor
- Intro to EE - The first thing we were taught
  - How a meter works
    - Panther Hollow and frogs
    - Magnets,windings, and deflection of an armature
    - Impedance, Calibration, Precision, Accuracy
  - Everything starts with measurement
- How do we measure which digital things?
  - Calibration? Precision? Accuracy?
- How do we measure protection?

# 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 about a general principal
    - Hypothesize $C \rightarrow^{M} E$
    - Perform experiments (e.g., $C \rightarrow^{M} \sim E$) 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

# Experiments and measurement

- We can't experiment without measurement
  - We must be able to measure E as a precursor to doing any experiment for causality
  - Unique measurement for each experiment is problematic
    - It lacks the scientific notion of a theory
    - It cannot be tested and is not repeatable
  - For science to advance, we must
    - Agree on the system of measurement
    - Be able to apply it to repeat experiments
      - Predict defined outcomes before testing
    - Be able to use it to confirm or refute hypotheses
      - Definitively compare measured to hypothetical results

# Metrics and measurement

- Different commonly recognized metrics classes
  - Nominal (Boy or Girl?)
    - Categories as non-overlapping sets
    - Supports set membership (=,≠)
  - Ordinal ([Major, Colonel, ...] [hate, like, love])
    - Ordered (ranked/partial) not equidistant
    - Supports non-arithmetic comparison (<,>,≤,≥,=,≠)
  - Interval ([1-5, 6-9, 10-30, 31 and up])
    - Ordered in equidistant scales in ranges
    - Supports limited arithmetic (+, -, <, >, ≤, ≥, =, ≠)
  - Ratio ([12/15], [298 degrees Kelvin])
    - Ordered, equal distance, true zero
    - Supports full arithmetic (+, -, *, /, <, >, ≤, ≥, =, ≠)

# Metrics and measurement

- A useful scientific scale must
  - Be well defined and agreed upon
  - Be repeatably usable for multiple purposes
  - Be experimenter independent
  - Differentiate between predicted outcomes
  - Be used to confirm/refute hypotheses w/in limits
- Example predictions:
  - Good for scientific use: Fewer children will be in the classroom after school than during school
  - Bad for scientific use: You will meet someone wonderful who likes you

# Example science

- Hypothesis: The World is flat
- Experiment: Keep sailing west
  - See if you come back from the east (nominal)
  - 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 house?
    - Or do you assume the Earth is flat?

# Some simple protection questions

- What is the definition of risk? (metric type?)
  - What are its units?
  - What is the standard of measurement?
  - Is it an absolute quantity?
- What can we do about it? (nominal)
  - 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?

Management Analytics

# Outline

- My background
- Measurement and science
- The human reality of science and protection
- The physics of digital information
- The future

# 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 enough will be checked
    - Once you lie in science - nobody will likely believe you again – and your old work will be largely discounted

# Important enough?

- We have created a highly dependent society
  - Advanced society may literally collapse without properly functioning information technology
- I care – but if you don't...
  - 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
  - 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?

# Did I mention what I do?

- Information protection involves people
  - Some people are malicious, intelligent, self-confident, highly adaptive, well educated, highly skilled and funded, physically fit, attractive, etc. And some teams of people combine these things together effectively
  - Other people are naïve, honest, gullible, lonely, tired, insecure, hurting, etc. And some of those people are highly trusted.
- What do you think happens when we pit some people against other people?
  - Can we predict the future? (science or magic?)

# Human behavior

- Personality testing – The Big 5 (Likert scale)
  - Openness to experience {inventive, curious} x {consistent, cautious}: Fantasy, Aesthetics, Feelings, Actions, Ideas, Values
  - Neuroticism {sensitive, nervous} x {secure, confident}: Anxiety, Hostility, Depression, Self-Consciousness, Impulsiveness, Vulnerability to Stress
  - Extraversion {outgoing, energetic} x {solitary, reserved}: Warmth, Gregariousness, Assertiveness, Activity, Excitement Seeking, Positive Emotion
  - Agreeableness {friendly, compassionate} x {cold, unkind}: Trust, Straightforwardness, Altruism, Compliance, Modesty, Tendermindedness
  - Conscientiousness: {efficient, organized} x {easy-going, careless} Competence, Order, Dutifulness, Achievement Striving, Self-Discipline, Deliberation

# Personality links to behavior

- Theory associates "personality" with behavior
  - People who commit certain types of crimes tend to have higher/lower ratings (percentile scores on big 5) in combinations of areas than others
  - But just because someone tests as being inventive/curious, easy-going/careless, outgoing/energetic, friendly/compassionate, and secure/confident doesn't mean they are a fraudster – or they may be
- Correlation is not causality
  - But how would we even measure correlation?
    - The Big 5 test is extensive and time consuming and cannot be forced on people often – or even once...

# Measuring personality

- Personal communications produce text
  - A hypothesis that word usage correlates to personality traits has been proposed
  - Testing shows correlation with the big 5
- But how might we use this?
  - Word usage correlates with personalities that correlate with undesired activities, so use the word usage as an indicator
- Mighty thin...
  - But there's more... aggravating factors (e.g., stressors), deceptive terms and phrases, ...

# What really happens?

- We don't know how to predict the future
  - At least not very well... until we do scientific experiments... and even then...
- The social sciences
  - The hard sciences are the easy sciences
  - The soft sciences are the hard sciences
- How do we measure people?
  - There is a theory of measurement for the social sciences
  - Good, bad, or otherwise, it provides a basis for comparison

# When I was not so young...

- 1983 – Deception in attack: computer viruses
  - Computer viruses don't have to be deceptive...
    - Most are: Trojan horses with reproduction and harm
    - Like other life forms, survival involves deception
- 1992 – Deception for defense
  - “An Evening with Berferd”
  - “OS protection through program evolution”
    - Evolve the OS s.t. each OS instance takes complex operations to “infect” → complexity leverage
- 1998 – “A Note on the Role of Deception in Information Protection”
  - Deception ToolKit (DTK) + a theory of deception
- 2001 - “A Framework for Deception”

# Info Pro Big Problems

- There are almost no scientific experiments
  - No widely used theory of measurement
  - Almost no useful metrics
    - Progress in an 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

Management Analytics

# 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
    - Deception and counter-deception effects
    - User interfaces and reasonable expectations
  - Without addressing the human aspects, we are destined to fail to meet our protection objectives

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. 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) Contact the help desk at x2331 for further assistance

**Continue?**

YES | NO

# A cognitive error theory

- 2001 – A Framework for Deception
  - Humans make known types of cognitive errors
  - Deception induces and suppresses signals to induce specific cognitive errors
  - The result is predictable changes in behavior
  - $C \rightarrow^{M} E$
    - C: Induced and/or suppressed signals
    - M: Cognitive errors
    - E: Predicted behavioral changes
- Experiments have confirmed for many cases
- The same applies to computers, groups, ...

# Outline

- My background
- Measurement and science
- The human reality of science and protection
- The physics of digital information
- The future

Management Analytics

# How did some sciences form?

| Physics | Biology | Digital space |
|---|---|---|
| Observe nature | Observe nature | |
| Theorize (Newton) | T..(Microorganisms) | No higher theory |
| Test / generalize | Test / generalize | |
| Build reliably | Build reliably | Don't build reliably |
| Oops... refutation | Oops... refutation | Models problematic |
| Theorize (Quantum) | Theory (Genes) | Some models |
| Test / generalize | Test / generalize | Complexity issues |
| Build reliably | Build reliably | Mathematics (right) |

Time ↓ (Physics, Biology); Time ↑ (Digital space)

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 complex / unknown at minutia level
    - P(x) problematic
    - Measure what? How?

# Notions of a new approach

- Information physics: (IRB decisions required)
  - A "physics of digital information" level to reduce complexity and allow composition based on physics properties
  - A "behavioral science" component to address social factors associated with protection
  - Example: Deception experiments from ~2000
    - "Leading Attackers Through Attack Graphs with Deceptions" - 2002
  - Human and group dynamics taken into account
  - Measured progress in attack graphs with time
  - Differential effects of 3 types of "deceptions"

# 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

F. Cohen, “Digital Forensic Evidence Examination - 4th ed.”, ASP Press, 2012

# 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: $E \rightarrow C$ unique!!!
  - **Normal space "diverges" with time!**
    - **Effect implies unique cause**

# 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 interpret/present bit sequences with FSMs
    - How do we assess and present tool reliability?
    - How do we deal with human interpretation of output?
  - 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 tools?
      - In most cases, no basis is provided / cognition ignored
    - 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?
    - How about human interpretation of output?
  - 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?
    - How do I interpret the output?

# Outline

- My background
- Measurement and science
- The human reality of protection
- The physics of digital information
- The future

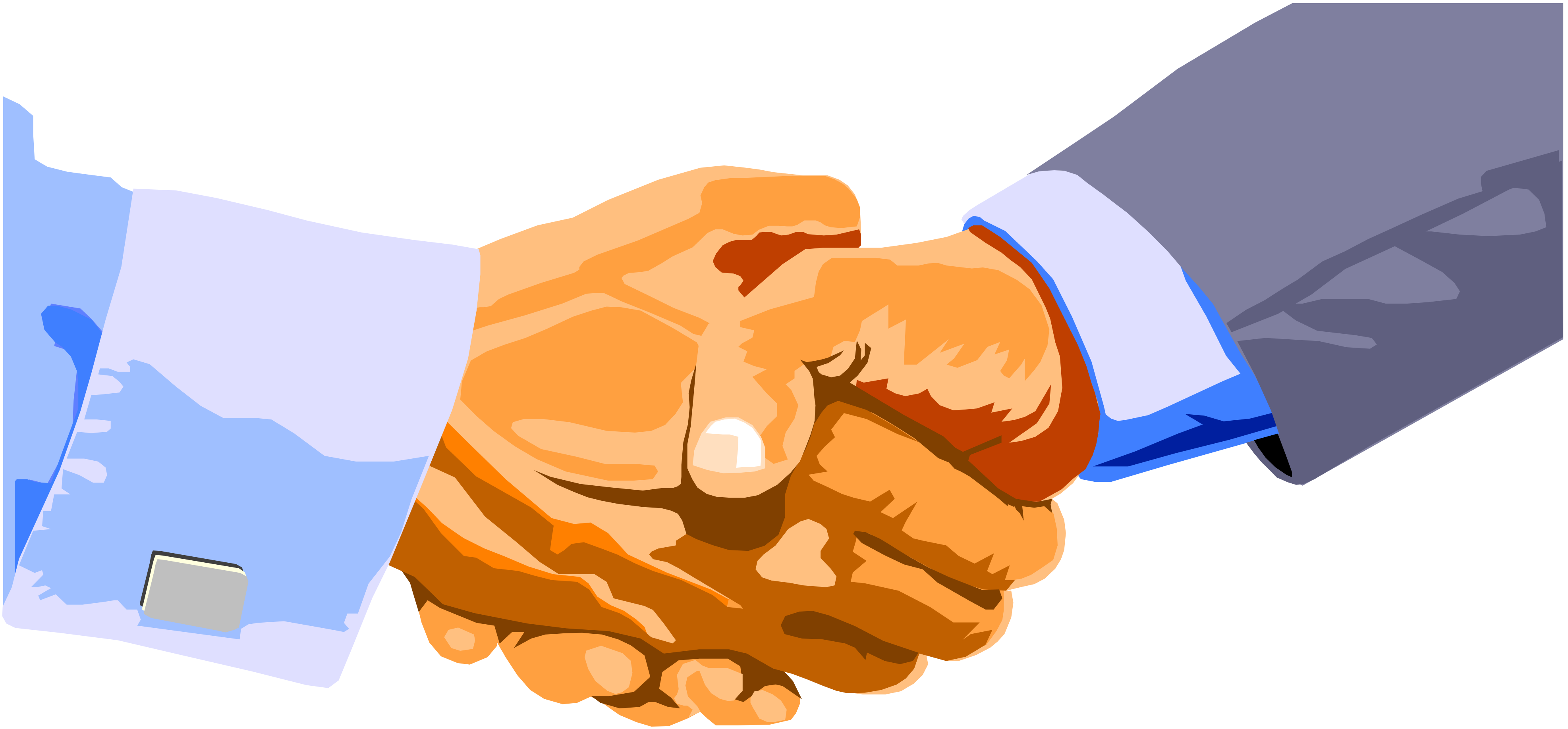
# An engineering discipline

- 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

# With social science included

- The social part of science... and engineering
- The successful discipline must account for computer, network, human, and group
  - Cognition, Behavior, Limits, Interaction, Personalities, Tolerances, Changes, Errors, Deception, Competition, Malice, Cooperation, Time frames, etc.
- Or...
  - We could continue to increase dependency on methodologies, systems, mechanisms, and people based on mysticism and hyperbole

# Thank You



**http://all.net/ - fc at all.net**