Can we do Better?

Science, Security, and the Elusive Science of Security

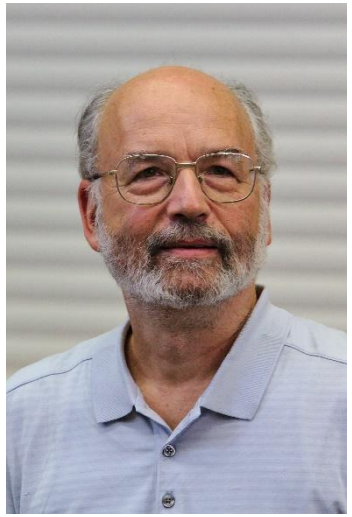
Cormac Herley

Microsoft Research, Redmond

- Unfalsifiability of security claims, Proc. Nat. Acad. Sciences
- Science, Security & Science of Security, IEEE S&P

“Non-crypto security will remain a mess.”

A. Shamir, Ten year predictions, 2002.



UK's cyber-security chief

www.independent.co.uk/news/uk/politics/uk-cyber-security-chief-gchq-internet-passwords-guidelines-ciaran-martin-national-...

INDEPENDENT

News InFact Politics Voices Indy/Life

News › UK › UK Politics

UK's cyber-security chief ridicules public guidelines for internet passwords as impossible even for spies to follow

Every British citizen is effectivel
Martin warns

Joe Watts Political Editor | @JoeWatts_ | Tue

32 shares

https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

The Man Who Wrote Those...

File Edit View Favorites Tools Help

DOW JONES, A NEWS CORP COMPANY

DJIA ▲ 21832.39 0.36% S&P 500 ▲ 2466.09 0.34% Nasdaq ▲ 6393.85 0.29% U.S. 10 Yr ▼ -11/32 Yield 2.099% Crude Oil ▲ 49.14 0.99% Euro ▲ 1.1923 0.07%

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

$1 for 2 Months

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate Search

A-HED

The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!

Bill Burr's 2003 report recommended using numbers, obscure characters and capital letters and updating regularly—he regrets the error

By Robert McMillan

Aug. 7, 2017 12:41 p.m. ET

The man who wrote the book on password management has a confession to make: He blew it.

Back in 2003, as a midlevel manager at the National Institute of Standards and Technology, Bill Burr was the author of "NIST Special Publication 800-63. Appendix A."

Some things claimed to be necessary are impossible

Portfolio of passwords:

1: Passwords should be random and strong

2: Passwords should not be re-used across accounts

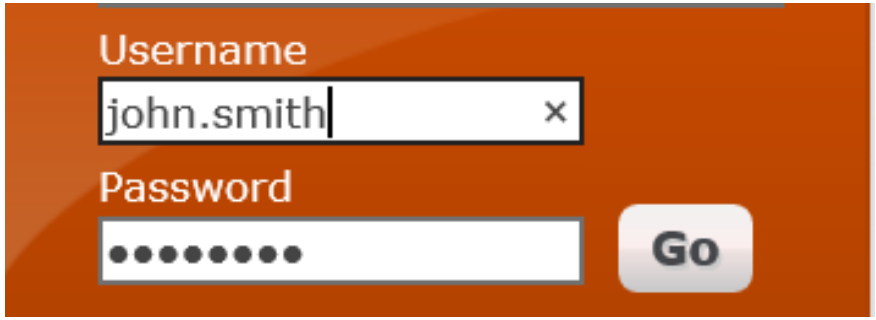
Suppose N=100 accts @ 40 bits/password:

$$N \cdot \lg(S) + \lg(N!) = 4000 + 524 = 4{,}524 \textit{ random} \text{ bits}$$

Equiv. to memorizing: 1361 places of pi, order of 17 packs of cards

……

Password Masking



Stop Password Masking

by **JAKOB NIELSEN** on June 23, 2009

Topics: Technology User Behavior

Summary: Usability suffers when users type in passwords and the only feedback they get is a row of bullets. Typically, masking passwords doesn't even increase security, but it does cost you business due to login failures.

- Schneier (June 26, 2009): “I agree with this”
- Epic flamewar in blogosphere
- Schneier (July 3, 2009): “So was I wrong? Maybe. Okay, probably”

How would we decide this question?

Why?

Why are we unable to answer a simple Y/N question about efficacy?

Why do we end up insisting on the necessity of things that are provably impossible (with 30s of arithmetic)

Password rules: biggest mass delusion in history?

Can we do Science/Security is special

What do we mean by Science?

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

Security is special

- Active adversary
- Relatively new field

Overview:

1) Science offers no path to certainty
2) Feedback is the engine of improvement
3) Feedback requires focus on the error/uncertainty
4) Anything that obscures the error, or impedes feedback retards progress

Science offers no path to certainty

Math/Formal Approaches

- Certain
- Proved true from axioms
- Cannot describe real world

Data/Empirical Approaches

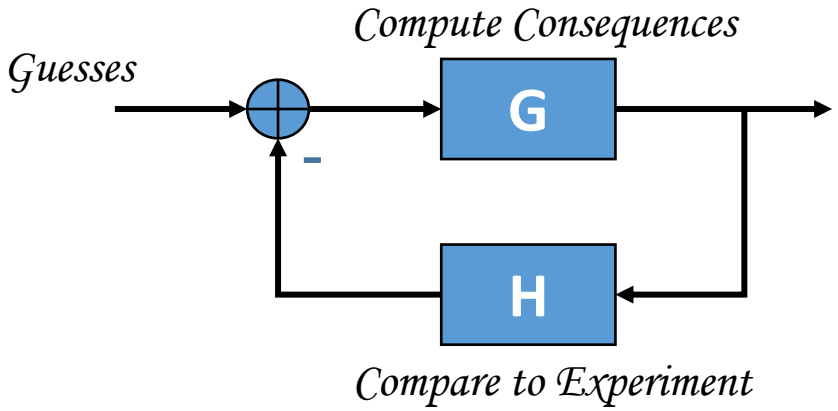
- Always uncertain
- Empirically supported falsifiable claims
- Describes real world

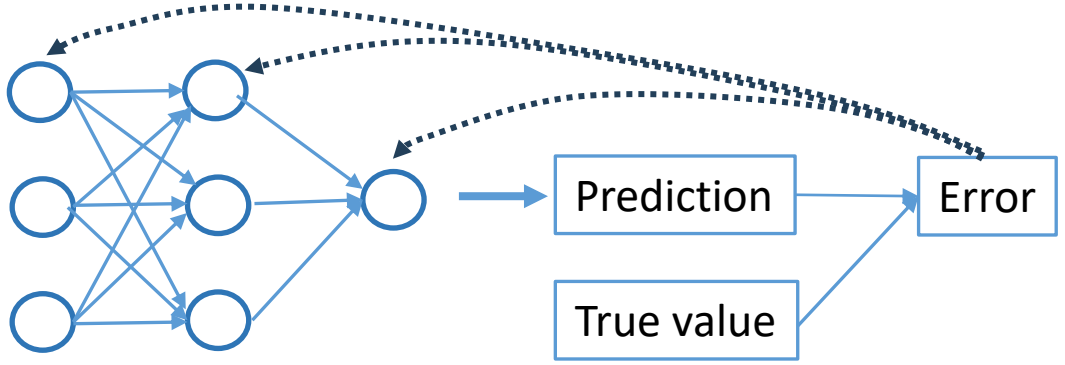
Each has a fundamental problem:

- Formal: ***require*** assumptions about real world
  - Proof + assumptions ≠ Proof
- Empirical: ***require*** generalization
  - Observation + argument about generality ≠ Law

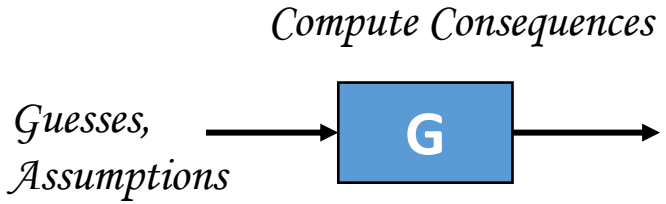
Feedback is the engine of improvement

"We guess laws. Then we compute the consequences of the guess, […] to compare it directly with observations to see if it works. If it disagrees with experiment, it's wrong. In that simple statement is the key to science." Feynman





The alternative:



Anything that obscures error/uncertainty impedes progress

Types of Error

- Conflict with observation
- Inconsistency
- Over-constrained
- Redundancy

Ways of obscuring

- Unfalsifiable
- Vague claims
- Over claiming
- Implicit assumptions
- Delay

Meanwhile, in Computer Security……

- **“The only secure system is unplugged, encased in concrete and buried at sea.”**
- **“What percent of the Fortune 100 have been hacked? 100%”**
- **“There are only two kinds of people: those who've been hacked and those who just don't know it yet.”**

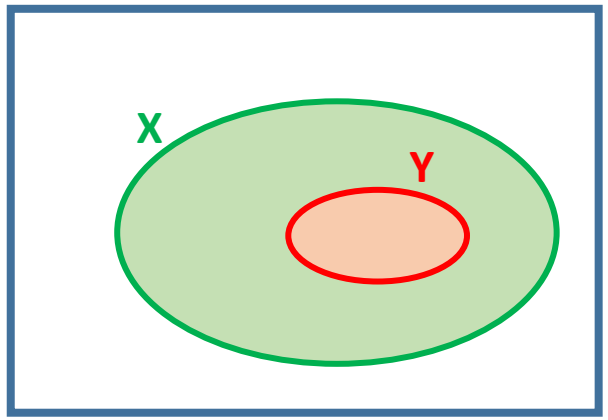
Can't observe security => Claims of insecurity or necessary conditions for security are unfalsifiable

Want x to be secure. Define $\mathbf{Y}$:

$$x \in \begin{cases} \mathbf{Y} & \text{is secure} \\ \overline{\mathbf{Y}} & \text{not secure.} \end{cases}$$

Falsifying "X is necessary for security" requires observing something secure that doesn't do X.

X is necessary for Y
equiv. $\mathbf{X} \supset \mathbf{Y}$
equiv. $\overline{\mathbf{X}} \Rightarrow \overline{\mathbf{Y}}$

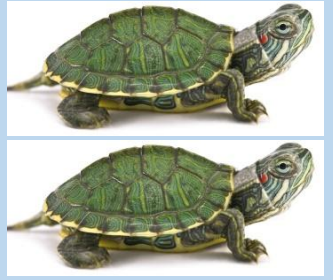


Claim: no observation falsifies $\mathbf{X} \supset \mathbf{Y}$.

Proof: to falsify $\mathbf{X} \supset \mathbf{Y}$ must show $\overline{\mathbf{X}} \cap \mathbf{Y}$ is not empty.

But can't find $x \in \mathbf{Y}$. ■

1. Security by threat model?



"Secure" if threat goals met: $\{X_0, X_1, X_2, \ldots, X_{N-1}\}$.

$$\mathbf{Y}_g \triangleq \cap_i \mathbf{X}_i$$

We ***can*** find members of $\mathbf{Y}_g$

Claim that:

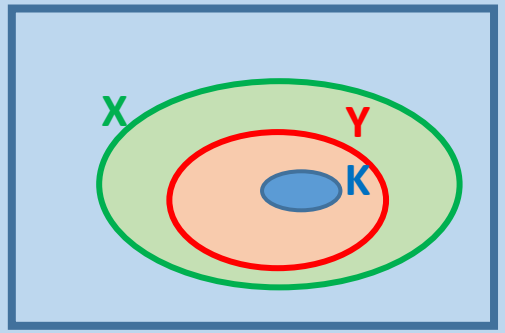
- $\mathbf{Y}_g$ sufficient (i.e.$\mathbf{Y}_g \subset \mathbf{Y}$) is falsifiable [find $x \in \mathbf{Y}_g \cap \overline{\mathbf{Y}}$]
- $\mathbf{Y}_g$ necessary (i.e. $\mathbf{Y}_g \supset \mathbf{Y}$) not falsifiable [find $x \in \overline{\mathbf{Y}_g} \cap \mathbf{Y}$]

- That goals are sufficient is falsifiable, but claim that necessary is not

2. Insecurity is the *possibility* of bad outcomes?

Define $\mathbf{K}$:

$$x \in \begin{cases} \mathbf{K} & \text{bad outcomes cannot happen} \\ \overline{\mathbf{K}} & \text{otherwise.} \end{cases}$$



Everything that cannot happen will not happen: $\mathbf{K} \subset \mathbf{Y}$

A subset of $\mathbf{Y}$ is no help in finding a superset of $\mathbf{Y}$

"Bad outcome possible
means
bad outcome will happen"

equiv. $\mathbf{K} \Rightarrow \mathbf{Y}$ means $\overline{\mathbf{K}} \Rightarrow \overline{\mathbf{Y}}$

aka: denying the antecedent

3. Security isn’t binary?

Without metric how do we falsify:

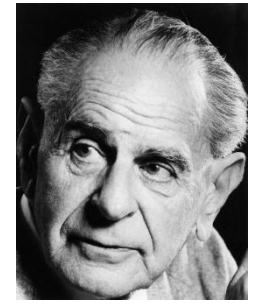
$$\text{Security}(\mathbf{X}) > \text{Security}(\overline{\mathbf{X}})$$

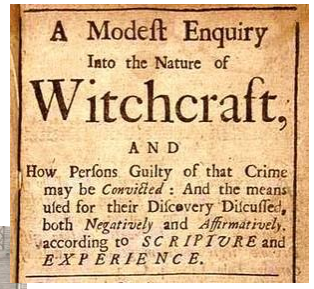
Unfalsifiable for all X

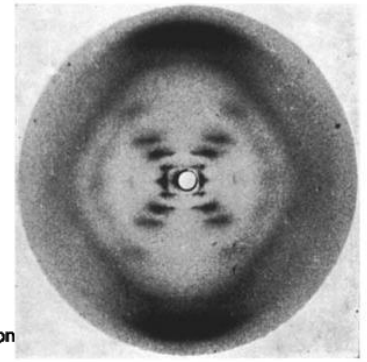
if (you don't do X) then: { **you are not secure** / **a bad outcome will occur** / **a bad outcome can occur** }

$$\text{Security}(\mathbf{X}) > \text{Security}(\overline{\mathbf{X}})$$

Is Computer Security a Pseudo-Science?

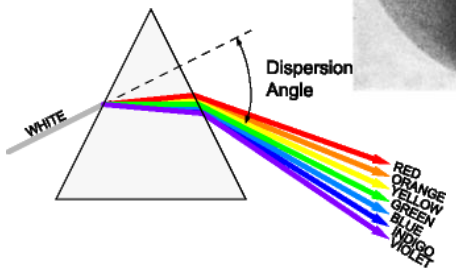


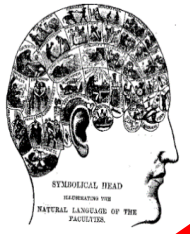


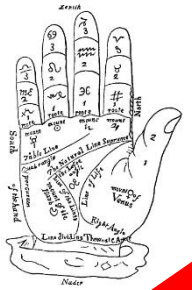


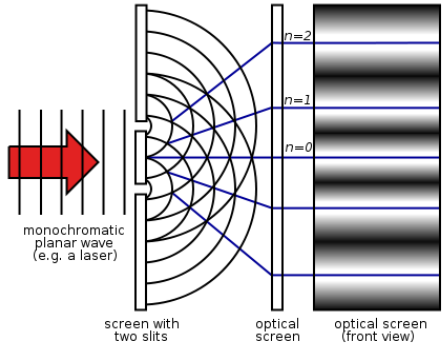
Your password must meet the following guidelines:

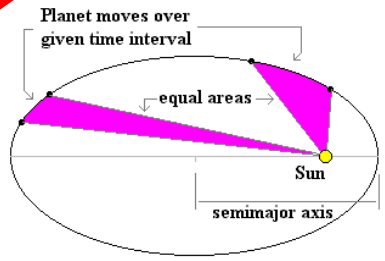
- be at least 8 characters and no more than 20
- contain one number from [0 - 9]
- contain one lowercase letter [a - z]
- contain one uppercase letter [A - Z]
- contain one of these special symbols: ! @ # $ % ^ & * ( ) + ?

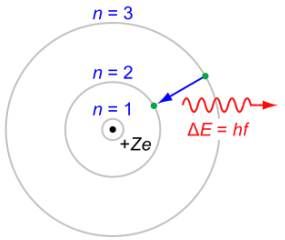












OK, OK, OK, we didn't mean this *literally*

When we say:

$$\text{Security}(\mathbf{X}) > \text{Security}(\overline{\mathbf{X}})$$

We actually mean, e.g.

$$\text{Outcome}(\mathbf{X}|\text{ABCD}) > \text{Outcome}(\overline{\mathbf{X}}|\text{ABCD})$$

For assumptions A, B, C, D ……

$$\text{Security}(\mathbf{X}) > \text{Security}(\overline{\mathbf{X}})$$

versus

$$\text{Outcome}(\mathbf{X}|\text{ABCD}) > \text{Outcome}(\overline{\mathbf{X}}|\text{ABCD})$$

Obscuring the error:

1. Expanded scope/Over-claiming
2. Forgotten/implicit and vague assumptions
3. Justification for X rests on plausibility/scope of ABCD

Self-Correction becomes one-sided :

new attacks argue counter-measures in, nothing can argue one out

Assume attacker capabilities →C = $\{c_0, c_1, c_2, \ldots, c_{N-1}\}$

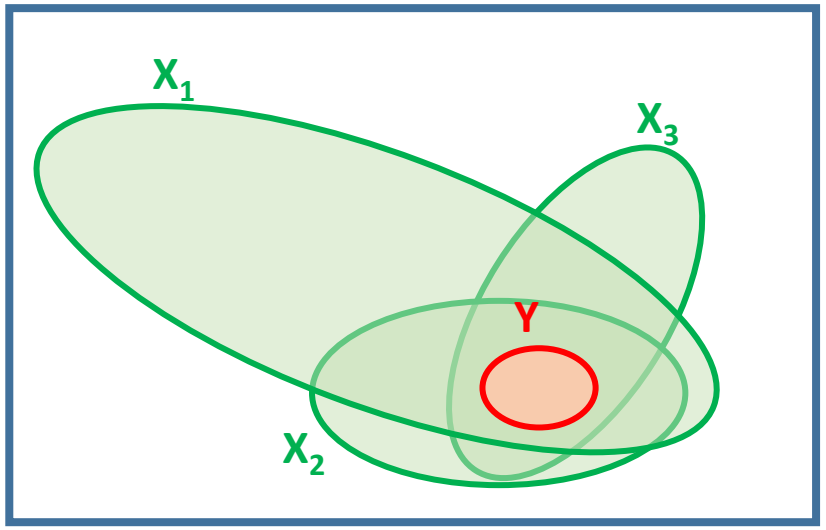
Collection of defensive measures M = $\{X_0, X_1, X_2, \ldots, X_{N-1}\}$

- **M not *sufficient* clear when new attack "steps outside" model**
- **M not *necessary* is not falsified by any possible observation.**

Confusing sufficient for necessary:
→ Over-constrained problems

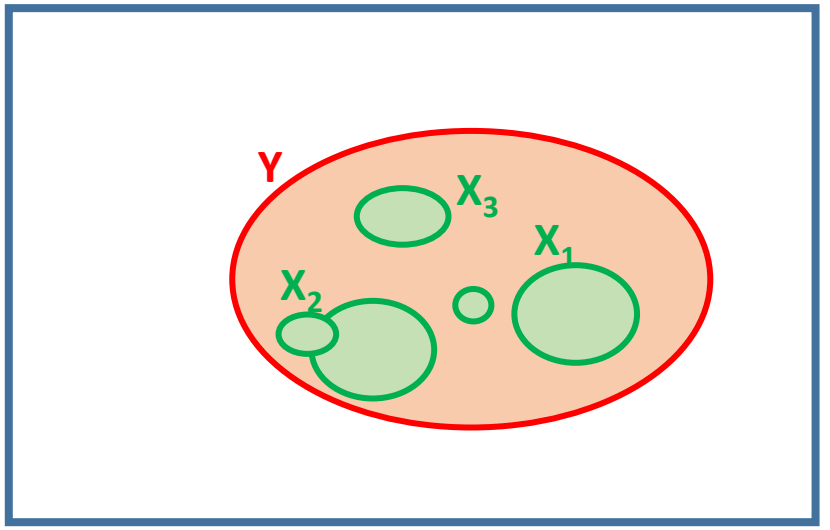
Simultaneous ***necessary*** conditions:

$$\bigcap_i \mathbf{X}_i \supset \mathbf{Y}$$



Simultaneous ***sufficient*** conditions:

$$\bigcap_i \mathbf{X}_i = \phi$$



Example over-constrained problem:

- Avoiding pwd re-use is sufficient to counter some attacks; but impossible to achieve across N=100 portfolio

Overview:

1) Science offers no path to certainty
2) Feedback is the engine of improvement
3) Feedback requires a clear view of the error
4) ***Anything that obscures the error, or impedes feedback retards progress***

Anything that obscures the error, or impedes feedback retards progress

- Can't measure or detect 'security' → structural unfalsifiability

- Implicit/obscured assumptions

$$\text{Security}(\mathbf{X}) > \text{Security}(\overline{\mathbf{X}})$$

versus

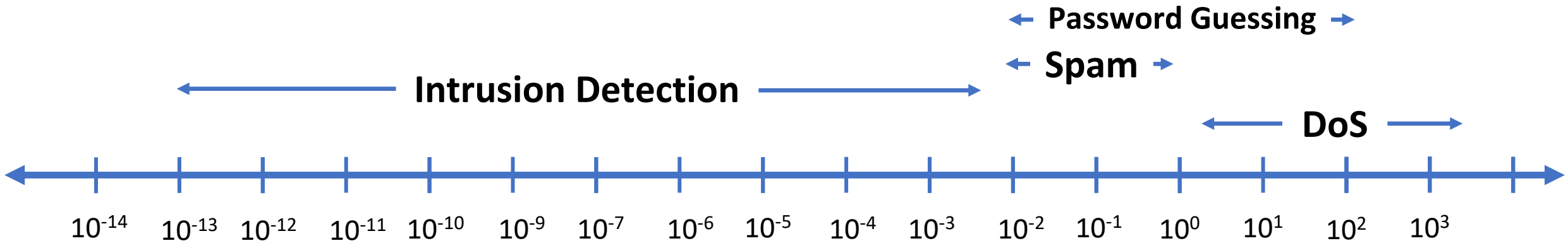
$$\text{Outcome}(\mathbf{X}|\text{ABCD}) > \text{Outcome}(\overline{\mathbf{X}}|\text{ABCD})$$

- Morris & Thompson, 1979

Feedback. Feedback. Feedback.

- ***If no data gives feedback on your theory: you don't have a theory, you have a religious belief***

- ***If your data doesn't give feedback on some theory: you don't have data, you have noise.***



- When data is sparse iterative feedback is harder
- Obscuring/denying the uncertainty is harmful

Conclusions

- Problem with the way we reason about problems
  - Unfalsifiable Claims,
  - Confusing sufficient for necessary
  - One-sided correction
  - Over-claims
- Feedback, feedback, feedback.
  - More rigor + more data doesn't solve the problem
- Progress requires clear view of uncertainty
  - Obscuring, denying is the wrong direction
- Generalization is impressively hard
  - "You can imagine a situation where……."
- Special pleading goes nowhere.
  - There's no other show in town.